International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Mitigating E-Commerce Fraud Through Consumer Awareness and Trust-Building: Insights into Vulnerability and Protection Strategies

Saritha Crasta[1], Dr. Caroleena Janefer[2]
[1]Assistant Professor, [2]Associate Professor, St. Aloysius (Deemed to be University), Mangaluru, India

***Abstract*-- The rapid expansion of e-commerce in Dakshina Kannada district has transformed consumer behavior, offering convenience and accessibility while simultaneously increasing exposure to online fraud. This study examines how consumer awareness, trust, and vulnerability interact to influence susceptibility to e-commerce fraud and identifies effective interventions to mitigate such risks. Employing a descriptive and exploratory design, a mixed-method approach was used with 200 online shoppers and 10 semi-structured interviews across the district. Purposive and convenience sampling guided data collection through structured questionnaires and interviews, supported by secondary data from journals and reports. The framework integrates Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Trust Theory to explain online consumer decision-making.**

Findings reveal that limited awareness and overconfidence significantly increase vulnerability, especially among younger consumers, while higher digital literacy and proactive habits reduce susceptibility. Fraud incidents cause both financial losses and psychological distress, diminishing trust and discouraging future digital engagement. The study calls for collaboration among government agencies, financial institutions, and e-commerce platforms to enhance digital literacy, promote transparency, and strengthen consumer protection mechanisms in Dakshina Kannada district.

***Keywords*- Consumer awareness, cybercrime prevention, digital trust, digital literacy, E-commerce fraud, fraud mitigation, online vulnerability, online security**

I. INTRODUCTION

E-commerce has revolutionized consumer-business interactions, providing unmatched convenience, variety, and affordability. However, the same digital transformation enabling this growth has also created new opportunities for fraudulent practices such as phishing, fake seller accounts, payment gateway manipulation, and counterfeit listings—posing major risks to consumers.

In Dakshina Kannada district of Karnataka, increasing internet connectivity, education, and digital payment use have spurred a surge in e-commerce activity. Yet, awareness about online security has not kept pace.

Many consumers continue to shop via mobile apps and social media markets without understanding security threats. The region's demographic diversity—comprising urban professionals, students, and rural users—adds behavioral complexity. Younger consumers frequently make impulsive purchases through social media ads, while older users remain skeptical or depend on others for online transactions.

Despite India's national focus on digital transformation, limited research examines how regional consumers perceive and respond to e-commerce fraud. Existing studies largely focus on metropolitan populations, overlooking semi-urban areas like Dakshina Kannada where rapid digital adoption coexists with weak consumer protection mechanisms. This study addresses that gap by analyzing awareness, vulnerability, and trust among online shoppers in the district.

The research is significant both theoretically and practically. Academically, it applies PMT, TPB, and Trust Theory to a regional Indian context, exploring behavioral determinants of fraud vulnerability. Practically, it provides insights for policymakers, educators, and businesses to design localized digital safety initiatives. Ultimately, the study seeks to enhance understanding of how awareness and trust-building can collectively strengthen consumer protection and promote safer e-commerce engagement in Dakshina Kannada district.

II. RESEARCH METHODOLOGY

A. Research Design and Population

The study followed a descriptive and exploratory research design to assess awareness, vulnerability, and trust among e-commerce users in Dakshina Kannada district. The population comprised active online shoppers from varied demographic and socioeconomic backgrounds.

B. Sampling and Data Collection

Using purposive and convenience sampling, primary data were collected from 200 survey respondents and 10 semi-structured interviews.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Structured questionnaires using a five-point Likert scale measured awareness, vulnerability, and trust. Interviews explored deeper behavioral insights, while secondary data came from academic journals, reports, and official publications.

C. Ethical Considerations

Informed consent was obtained from all participants, and confidentiality was strictly maintained. No identifiable personal data were disclosed.

D. Theoretical Framework

The research draws on three behavioral theories:

Protection Motivation Theory (PMT): Individuals adopt protective behaviors when they perceive high threat severity and personal vulnerability.

Theory of Planned Behavior (TPB): Intentions to engage in safe online behavior are shaped by attitudes, subjective norms, and perceived behavioral control.

Trust Theory: Trust lowers perceived risk in digital transactions and sustains long-term consumer participation.

III. Literature Review

Existing literature highlights that the rapid expansion of e-commerce has been accompanied by a parallel rise in sophisticated online fraud, significantly affecting consumer trust and participation in digital markets. Studies consistently report that phishing, fake seller accounts, counterfeit products, and payment fraud are among the most prevalent threats undermining consumer confidence (Knuth & Ahrholdt, 2022; Sharma et al., 2024). Research grounded in Protection Motivation Theory (PMT) suggests that consumers' adoption of protective behaviors depends largely on perceived threat severity, vulnerability, and coping efficacy; however, many online shoppers underestimate personal risk, resulting in weak preventive action (Gupta et al., 2017; Lonkar et al., 2024). This gap between awareness and behavior is particularly evident among younger consumers, who display high digital engagement but greater susceptibility due to impulsive purchasing and overconfidence (Parveen & Krishnaraj, 2024).

Further studies emphasize that trust plays a central role in sustaining e-commerce adoption, with fraud incidents leading to long-term psychological distress, avoidance of digital platforms, and preference for cash-based transactions (Adnan et al., 2023; Marwi & Oskar, 2023).

Trust Theory explains that once institutional or platform trust is breached, rebuilding confidence requires visible security assurances, transparent communication, and effective redressal mechanisms. Complementing this, the Theory of Planned Behavior (TPB) demonstrates that attitudes toward online safety, subjective norms, and perceived behavioral control significantly influence consumers' intentions to adopt secure online practices (Ahmad & Simpao, 2024). While prior research provides valuable insights into fraud dynamics, most studies focus on metropolitan or national-level contexts, leaving semi-urban regions underexplored. This study addresses this gap by examining consumer awareness, vulnerability, and trust in Dakshina Kannada district, offering region-specific insights into behavioral and institutional strategies for mitigating e-commerce fraud.

IV. Findings And Analysis

A. Consumer Awareness

Most respondents possessed only basic knowledge of e-commerce fraud types such as phishing and fake seller accounts. Awareness of advanced threats like spoofed gateways or malware-laden ads was limited. In PMT terms, this reflects low threat appraisal—consumers acknowledge risks but underestimate their personal vulnerability, reducing motivation for preventive action.

B. Perceived Vulnerability

Despite good internet literacy, most respondents felt vulnerable due to increasingly sophisticated scams, including AI-generated advertisements and fake brand impersonations. Younger consumers (18–30 years) were confident but overexposed due to impulsive purchases via social media, while older users lacked technical proficiency and avoided advanced security features.

C. Financial and Psychological Impacts

Fraud incidents resulted in losses ranging from ₹500 to ₹20,000, often through fake ads, counterfeit goods, or unauthorized transactions. Victims also suffered embarrassment, anxiety, and social stigma, leading to temporary withdrawal from online shopping. According to Trust Theory, once consumer trust is violated, regaining confidence requires sustained institutional reassurance.

D. Erosion of Trust in Platforms

Consumers who experienced fraud exhibited significant distrust even toward major e-commerce companies.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Respondents distinguished between platform trust (e.g., Amazon, Flipkart) and seller trust, showing more skepticism toward third-party or social media-based sellers. Visible security signals—such as verified seller badges and refund guarantees—were perceived as effective in restoring confidence.

E. Institutional Gaps

Respondents reported inadequate institutional support and limited awareness of grievance mechanisms. Those who complained faced delayed responses and poor redressal. Weak coordination among banks, cybercrime units, and e-commerce platforms was a recurring concern, underscoring the need for integrated fraud response systems.

F. Generational Differences

18–30 years Tech-savvy but overconfident and impulsive. 31–45 years: Moderately aware but inconsistent in security practices.

46+ years: Cautious but digitally underprepared, relying on family assistance.

This suggests the need for age-specific awareness interventions—community-based training for older adults and behavioral nudges for younger consumers.

G. Social Media as a Fraud Channel

Social media platforms like Instagram, Facebook, and WhatsApp emerged as leading gateways for scams, with fake promotions and counterfeit product ads exploiting influencer credibility. Fraud is shifting from traditional e-commerce websites to decentralized, ad-driven ecosystems with weak oversight.

H. Reactive Consumer Behavior

Most respondents adopted safety measures only after encountering fraud or learning of others' experiences, indicating reactive rather than preventive behavior. Under PMT, this reflects low coping appraisal—individuals acknowledge risk but perceive prevention as inconvenient or unnecessary until personally affected.

I. Platform Trust Variations

Trust was highest in established platforms and lowest in small or unregulated ones. While brand reputation offers perceived safety, overreliance on a few major players can limit market diversity, highlighting the need for standardized industry-wide fraud prevention protocols.

V. RECOMMENDATIONS

A. Enhancing Awareness and Digital Literacy

District-Level Campaigns: Conduct periodic workshops via schools, NGOs, and local government offices to educate on fraud types and safe practices.

B. Curriculum Integration:

Include digital safety and fraud prevention in school and college courses to shape attitudes early, aligning with TPB principles.

C. Localized Media Outreach:

Disseminate safety messages through regional TV, radio, and social media in local languages.

D. Inclusive Training:

Provide simplified, visual literacy programs for older adults and rural users.

E. Strengthening Consumer Protection Mechanisms

Establish a 24/7 fraud helpline with quick response systems.

Implement transparent complaint portals and mandated resolution timelines. Introduce compensation policies for verified victims and provide counseling support for psychological recovery.

F. Building and Sustaining Trust

Launch verified seller programs and buyer protection guarantees on all platforms. Promote platform transparency by publicly communicating data protection and refund policies. Encourage post-fraud engagement by offering victims educational follow-ups to rebuild confidence.

G. Institutional and Regulatory Reforms

Strengthen collaboration between cybercrime units, banks, and e-commerce platforms for joint investigations. Update cyber laws to cover influencer-driven and social media-based scams. Require platforms to publish periodic fraud reports and collaborate with regulators for oversight. Regulate social media advertising to curb fake listings and ensure accountability.

H. Technological Measures

Implement AI-based fraud detection systems and real-time scam monitoring. Explore blockchain-based transaction verification for enhanced transparency. Mandate two-factor authentication for all e-commerce payments. Educate users on digital hygiene—password rotation, privacy settings, and secure browsing.

I. Community and Policy Integration

Form a district-level E-Commerce Fraud Monitoring Cell involving cyber experts and law enforcement.

Integrate consumer protection goals into Digital India and Smart City initiatives. Encourage public–private partnerships between universities (e.g., St. Aloysius Deemed to be University), local administration, and tech firms to run joint awareness drives and pilot prevention programs.

J. Theoretical and Practical Implications

This study reinforces the relevance of:

PMT: Heightened threat perception and coping efficacy encourage preventive actions.

TPB: Positive social norms and perceived control shape online safety habits.

Trust Theory: Transparency and reliability sustain long-term consumer confidence.

Practically, these measures can reduce consumer vulnerability, rebuild trust, and enable inclusive, secure digital growth in Dakshina Kannada district.

VI. Conclusion And Future Scope

Consumer awareness and trust are pivotal in mitigating e-commerce fraud. In Dakshina Kannada district, rapid digital adoption without parallel growth in awareness has heightened vulnerability, especially among overconfident young users and digitally untrained older consumers. Fraud incidents cause both financial and emotional harm, eroding confidence and slowing digital participation.

Rebuilding trust requires continuous collaboration among consumers, platforms, and policymakers. The study validates PMT, TPB, and Trust Theory, demonstrating that awareness enhances perceived control, reduces vulnerability, and strengthens digital trust.

Future studies could expand to other districts for comparative analysis or adopt longitudinal designs to examine the lasting impact of awareness programs. Experimental research could also test the effectiveness of gamified fraud-prevention training.

Ensuring secure digital participation demands balancing convenience with protection. By advancing digital literacy, institutional accountability, and transparent communication, Dakshina Kannada—and similar semi-urban regions—can cultivate safer, more resilient e-commerce ecosystems.

REFERENCES

[1] Adnan, A. M., Manap, N. A., & Zakaria, Z. (2023). Online purchase fraud cases: Business ethics versus consumer attitudes. *International Journal of Academic Research in Business and Social Sciences, 13*(6), 1021–1035. https://doi.org/10.6007/IJARBSS/v13-i6/17045

[2] Ahmad, F., & Simpao, K. J. (2024). E-commerce fraud perceptions and preventive measures: Evidence from Pakistan. *ITQAN Journal of Islamic Economics, 4*(1), 45–59.

[3] Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. *arXiv preprint arXiv:1705.04009*.

[4] Knuth, T., & Ahrholdt, D. C. (2022). Consumer fraud in online shopping: An empirical analysis of risk and trust. *International Journal of Electronic Commerce, 26*(3), 388–411. https://doi.org/10.1080/10864415.2022.2069694

[5] Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: Challenges and regulatory responses. *Journal of Financial Crime*. Advance online publication. https://doi.org/10.1108/JFC-2023-0214

[6] Marwi, H., & Oskar, I. (2023). Analysis of increasing types of online fraud in Indonesia. *Journal of Embedded Systems, Security and Intelligent Systems, 4*(2), 55–63.

[7] Parveen, S., & Krishnaraj, R. (2024). Vulnerability of Gen-Z to e-commerce deception: An analysis of consumer belief categories. *Quality Innovation Prosperity, 28*(2), 1–18. https://doi.org/10.12776/qip.v28i2.1832

[8] Renjith, S. (2018). Detection of fraudulent sellers in online marketplaces using support vector machine approach. *arXiv preprint arXiv:1805.03353*.

[9] Sharma, A., Chakraborty, P., & Kumar, V. (2024). Online monetary fraud analysis: Trends, detection, and prevention. *Journal of Informatics Education and Research, 4*(3), 112–124.

[10] Parveen, S., & Krishnaraj, R. (2024). Vulnerability of Gen-Z to E-Commerce Deception on Consumer's Belief Categories. Quality Innovation Prosperity, 28(2).

[11] Ahmad, F., & Simpao, K. J. (2024). E-Commerce Fraud Perceptions in Pakistan and Preventive Measures. ITQAN Journal of Islamic Economics, 4(1).

[12] Sharma, A., Chakraborty, P., & Kumar, V. (2024). Online Monetary Fraud Analysis. Journal of Informatics Education and Research, 4(3).

[13] Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2024). Tackling Digital Payment Frauds. Journal of Financial Crime.

[14] Knuth, T., & Ahrholdt, D. C. (2022). Consumer Fraud in Online Shopping. International Journal of Electronic Commerce, 26(3), 388–411.

[15] Marwi, H., & Oskar, I. (2023). Analysis of Increasing Types of Online Fraud in Indonesia. Journal of Embedded Systems, Security and Intelligent Systems, 4(2).

[16] Adnan, A. M., Manap, N. A., & Zakaria, Z. (2023). Online Purchase Fraud Cases: Business Ethics vs Consumer Attitudes. International Journal of Academic Research in Business and Social Sciences, 13(6).

[17] Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending Against Phishing Attacks. arXiv.

[18] Renjith, S. (2018). Detection of Fraudulent Sellers in Online Marketplaces Using Support Vector Machine Approach. *arXiv.*