International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

The Role of Digital Literacy in Strengthening Resistance to E-Commerce Fraud

Saritha Crasta[1], Dr. Caroleena Janefer[2], Ashlene Albuquerque[3]

[1]*Assistant Professor,* [2]*Associate Professor,* [3]*Student, School of Commerce, Finance and Accountancy, St. Aloysius (Deemed to be University), Mangaluru, India*

***Abstract*— Consumers today operate in a rapidly growing online environment and, along with unparalleled convenience and choice, a range of new threats have been posed by fraudsters: including phishing attacks, knockoff products, identity theft and fraudulent payments have all become a growing part of the online shopper's reality. Digital literacy, which is essentially skills in locating, evaluating and safely applying information and tools in the digital domain, plays an extremely important role in determining the ability of consumers to defend themselves from such fraudsters. This paper investigates the interaction of digital literacy and e-commerce fraud in the framework of Protection Motivation Theory (PMT). Protection Motivation Theory says that people will respond in order to protect themselves if they perceive a threat as serious and a method to deal with the threat exists. The research employs a descriptive design where data was obtained through a structured questionnaire and a random sample of 268 shoppers online completed. Data was analyzed through a descriptive correlation and regression analysis technique. Research found that digital literacy influences the consumers' threat appraisal, self-efficacy, and their response efficacy so they display a strong resistance to fraudsters. The results show that more digitally literate shoppers appear to be able to stick to practices to protect themselves such as making sure they are shopping on an appropriate website, securing their payment options and identifying attempts at phishing. The concluding section of the research discusses that there should be greater investment in developing training programs focused on digital literacy, further development of regulation measures and cooperation between online service providers, higher education institutions and public institutions.**

***Keywords*— Digital literacy, E-commerce fraud, Protection Motivation Theory, Consumer protection, Online safety, Fraud resistance, Self-efficacy,**

I. Introduction

E-commerce has emerged as a prominent force shaping the global economic landscape. Powered by the widespread adoption of smartphones, inexpensive internet access, and efficient digital payment systems, online shopping is now an integral part of the daily routine of millions of consumers. In India, the growth of e-commerce has been phenomenal, with countless transactions taking place every second across popular platforms like Amazon, Flipkart, Meesho, etc.

This revolution has fundamentally altered how people shop for goods and services, making it quicker, cheaper, and much more personalized.

However, there is a flip side to this digital progress. The same digital ecosystem that facilitates these seamless transactions also provides fertile ground for all kinds of fraudulent activities. Various forms of fraud, such as phishing, fake online stores, identity theft, payment fraud, and the sale of counterfeit products, have become excessive and increasingly sophisticated. Consumers who fall prey to these schemes suffer financial losses and lose their trust in digital spaces.

In this context, this paper draws on the Protection Motivation Theory (PMT), initially proposed by Rogers (1975), to better understand consumer resistance to e-commerce fraud. PMT implies that people are motivated to protect themselves against a threat when they assess its severity and likelihood (Threat Appraisal) and their abilities to take preventative action (Coping Appraisal). Digital literacy influences consumers' perception of the seriousness and likelihood of fraud, enhances perceived susceptibility, and promotes people's confidence in taking necessary measures to avoid the threat.

Henceforth this research investigates how digital literacy influences consumer resistance to e-commerce fraud under the framework of PMT. Furthermore, the study investigates whether consumers' digital skills are actually translated into consistently protective behavioral actions, and this finding may have a contribution to policy making of consumer education, online trading platform design and regulative methods towards safe online trading environments.

II. Literature Review

Digital Literacy and Online Consumer Behavior is perhaps one of the most researched competences related to the digital economy. Researchers often define it as: 'the ability to access, understand, evaluate and interact with information through digital technologies in a responsible and safe manner'. Most research suggests that as digital literacy increases, so does an individual's ability to avoid online risks.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

For instance, Li, Peng, and Du (2024) suggest that improving residents' digital literacy can help them avoid falling victim to fraud, such as in the case of online financial transactions and online shopping through a three-stage Probit model, where the findings confirm that digital knowledge will reduce fraud susceptibility among residents in the digital economy. Another publication, from 2025, also confirmed how digital literacy significantly determines perceptions, frequency of online purchasing behaviour and safety of consumers in relation to e-commerce.

Numerous fraudulent activities have been identified within the e-commerce sphere. Fake profiles, fake products, payment fraud, phishing, and account takeover and data breaches seem to be some of the most common issues for consumers in online shopping. Numerous scholars confirmed that online fraud will decrease online consumers' trust towards e-commerce websites, online purchase intentions, and future online engagements.

As Featherman and Pavlou (2003) established, online consumers will have difficulties in developing trust towards e-commerce websites, and in regaining that trust after a negative experience, because trust is an essential element that allows consumers to fully participate in the online economy and it will significantly influence consumer behaviours. Gefen et al. (2003) also demonstrate how trust is significant in determining user acceptance of technology and online shopping, especially where there is a level of risk and uncertainty, suggesting that it is the perceived security, not the actual one, that defines the trust a user may have in an e-commerce website.

Originally developed by Rogers (1975, 1983), Protection Motivation Theory (PMT) has often been utilised within research concerning cybersecurity and online safety. According to the theory, protection behaviour can be triggered by two cognitive appraisal processes: threat appraisal, which considers both vulnerability and the severity of the perceived threat, as well as coping appraisal, which considers the efficiency of coping response and self-efficacy of the individual. Using PMT to investigate Information Security Policy Compliance, Herath and Rao (2009) found that threat appraisal and coping appraisal both play a significant role in individuals' protection behaviour intentions. PMT was also utilised by Boerman, Kruikemeier and Borgesius (2021) to study online privacy protection behavior, where they established that response efficacy, in particular, has a role in prompting behavior change.

Perhaps the most enduring result emerging from research on online fraud is the 'awareness–action gap' in which individuals are aware of fraud and often how it works but do not put that awareness into practice.

Sheng et al. (2010) studied why users were vulnerable to phishing and found that overconfidence, lack of technological expertise and lowered attention are largely why people fall victim, suggesting that just awareness alone was not enough to prevent risky behavior. Khan et al. (2021) found that varying prevention behavior was also common in developing countries where access to technology and levels of security education may not be as prevalent. Boss et al. (2015) proved that adding fear appeals to a situation where users already felt confident in their ability to protect themselves significantly improved security behaviors.

The literature strongly points towards the requirement of a structured and actionable approach rather than just awareness programmes. Aloul et al. (2022) showed that consumer educational programmes improved fraud awareness and the likelihood of falling victim was decreased. From a legal perspective, recent work on e-commerce and consumer protection in India has emphasized the need for legislation such as the Consumer Protection Act, 2019 and Consumer Protection (E-Commerce) Rules, 2020 for implementing accountability on online platforms and ensuring efficient grievance redressal mechanisms (Chawla & Kumar, 2022; Bhangla & Tuli, 2021).

III. Objectives Of The Study

1. To examine the level of digital literacy among online shoppers and its influence on fraud awareness.
2. To assess the relationship between digital literacy and the adoption of fraud-preventive behaviors.
3. To analyze how Protection Motivation Theory constructs — threat appraisal and coping appraisal — mediate the link between digital literacy and fraud resistance.
4. To identify the key barriers that prevent digitally aware consumers from consistently adopting preventive practices.
5. To provide practical recommendations for improving consumer resilience against e-commerce fraud through digital literacy enhancement.

IV. Research Questions

1. What is the current level of digital literacy among online shoppers, and how does it vary across demographic groups?
2. Does digital literacy significantly influence the level of fraud awareness and perceived threat among consumers?
3. How do PMT constructs — perceived severity, perceived vulnerability, response efficacy, and self-efficacy — relate to consumers' preventive behavior?

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

4. What barriers prevent digitally aware consumers from consistently practicing fraud-preventive behavior?
5. What role can educational institutions, e-commerce platforms, and regulatory bodies play in strengthening consumer digital literacy?

V. Methodology

The study adopts a descriptive research design with a quantitative research approach for collection of data through primary source with the help of a questionnaire among actively participating online shoppers. Respondents for the study were selected through convenience sampling method, i.e., among online users who routinely shop online on a regular basis through various shopping platforms.

A. Sample and Data Collection

A total of 285 questionnaires were distributed, of which 268 were found complete and suitable for analysis after data screening. The questionnaire was divided into five sections: demographic profile, digital literacy assessment, fraud exposure experiences, threat and coping appraisal (based on PMT), and preventive practices. A five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) was used for all perceptual measures.

B. Variables

The study incorporates the following key variables aligned with Protection Motivation Theory:

Digital Literacy: Ability to identify secure websites, recognize phishing indicators, use privacy settings, and evaluate online information critically.

Perceived Severity: The degree to which respondents believe e-commerce fraud can cause serious harm.

Perceived Vulnerability: The extent to which respondents feel personally at risk of falling victim to fraud.

Response Efficacy: Belief that protective measures such as two-factor authentication and verified payment gateways are effective.

Self-Efficacy: Confidence in one's personal ability to identify and avoid fraudulent situations.

Preventive Practices: Actions such as verifying websites, using secure passwords, enabling transaction alerts, and avoiding suspicious links.

C. Statistical Analysis

Data were coded and analyzed using SPSS. The following techniques were applied:

Descriptive Statistics: Mean, standard deviation, frequency, and percentage to summarize key variables.

Reliability Analysis: Cronbach's Alpha to assess internal consistency of constructs (threshold: $\alpha > 0.70$).

Correlation Analysis: To examine the relationships between digital literacy, PMT constructs, and preventive practices.

t-test: To compare preventive behavior between high and low digital literacy groups.

ANOVA: To assess variation across age, education, and gender groups.

Regression Analysis: To determine the predictive power of digital literacy and PMT constructs on fraud-preventive behavior.

All inferential tests were conducted at a 5% significance level ($p < 0.05$), with 1% significance ($p < 0.01$) noted where applicable.

VI. Data Analysis And Discussion

TABLE I
Descriptive Statistics and Reliability Analysis

Variable	Mean	SD	Interpretation	Cronbach's α
Digital Literacy	3.61	0.74	Moderately High	0.83
Perceived Severity	4.18	0.61	High	0.81
Perceived Vulnerability	3.35	0.89	Moderate	—
Self-Efficacy	3.78	0.69	High	0.86
Response Efficacy	3.52	0.77	Moderately High	—
Preventive Practices	3.44	0.82	Moderate	0.79

The descriptive results reveal that respondents show moderately high levels of digital literacy (Mean = 3.61) and a strong perception of fraud severity (Mean = 4.18). However, the actual adoption of preventive practices remains moderate (Mean = 3.44), suggesting that even among consumers with reasonable digital skills, there is an inconsistency between awareness and consistent protective action. Reliability values above 0.79 across all constructs confirm acceptable to good internal consistency.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

A. Correlation Analysis

TABLE II
CORRELATION MATRIX

Variable	1	2	3	4	5
1. Digital Literacy	1				
2. Perceived Severity	0.44**	1			
3. Self-Efficacy	0.58**	0.46**	1		
4. Response Efficacy	0.51**	0.43**	0.53**	1	
5. Preventive Practices	0.63**	0.47**	0.61**	0.44**	1

** $p < 0.01$

The correlation results demonstrate that digital literacy has the strongest association with preventive practices ($r = 0.63$, $p < 0.01$), more than any individual PMT construct alone. Self-efficacy also shows a strong correlation with preventive behavior ($r = 0.61$), confirming that consumers who feel capable of protecting themselves are more likely to take consistent action. Perceived severity, while positively correlated, shows a comparatively weaker relationship with actual behavior, reinforcing the well-established finding that knowing a threat is serious is not enough on its own to drive action.

B. Comparative and Regression Analysis

TABLE III
REGRESSION AND COMPARATIVE ANALYSIS

Test	Key Result	Interpretation
t-test (High vs Low Digital Literacy)	$t = 3.24$, $p = 0.001$	High literacy group significantly more preventive
ANOVA (Age)	$F = 4.12$, $p = 0.007$	Significant age-based variation
ANOVA (Education)	$F = 2.87$, $p = 0.038$	Significant education-based variation
ANOVA (Gender)	$F = 1.14$, $p = 0.286$	Not significant
Regression (R^2)	0.61	Model explains 61% of variance
Digital Literacy (β)	0.38, $p = 0.000$	Highly Significant
Self-Efficacy (β)	0.29, $p = 0.001$	Highly Significant
Response Efficacy (β)	0.18, $p = 0.024$	Significant
Perceived Severity (β)	0.14, $p = 0.041$	Significant

The regression analysis reveals that digital literacy ($\beta = 0.38$) is the strongest predictor of fraud-preventive behavior, followed by self-efficacy ($\beta = 0.29$). The overall model explains 61% of the variance in preventive practices, indicating strong explanatory power. The t-test confirms that respondents with higher digital literacy scores engage in significantly more preventive behaviors compared to those with lower scores. Education level also emerges as a significant differentiator, suggesting that formal education plays a meaningful role in building digital competence. Gender, however, shows no significant impact on preventive behavior.

C. Discussion of Findings

The results of this study suggest there is a significant and logical association between digital literacy and resistance to e-commerce fraud. Our results demonstrate that the more technologically skilled a consumer is, the better they are at identifying indicators of e-commerce fraud, the more self-confident they are to take measures against it, and the more consistently they adopt protective measures.

Within the PMT framework, this indicates that higher levels of digital literacy boost both threat appraisal (by making consumers better aware of fraud instances) and coping appraisal (by building response efficacy and self-efficacy against threats).

One interesting finding is the critical role that self-efficacy plays in moderating between knowledge and behavior: consumers who are aware of fraud and its risks but are unconfident in their ability to respond will likely not take defensive measures. In contrast, those who have learned about online fraud and also feel confident in their capacity to prevent it are much more likely to consistently undertake preventive action, and therefore should be directly trained through practical tasks that build both knowledge and efficacy.

Educational differences also provide interesting results that warrant special focus. Consumers who have achieved higher educational levels demonstrate higher levels of digital literacy and undertake more consistent defensive activities.

But the gap separating these higher-educated consumers from their lower-educated peers indicates that digital skills can hardly be taken as automatically attained, thus highlighting their development, particularly in less digitally educated consumers.

VII. Conclusion

The study sought to understand how digital literacy strengthens consumer resistance to e-commerce fraud, with the Protection Motivation Theory guiding the construction of the study. The findings supported that digital literacy is far from a general-purpose background skill; it is indeed instrumental in helping consumers anticipate, respond to, and resist various kinds of online fraud. Digitally literate individuals exhibited more perceived threat awareness, stronger self-efficacy and more proactive defensive behaviors in the online world. At the same time, the present study highlighted the critical existence of awareness–action gaps even for reasonably digitally literate users, and the inconsistent preventive behavior reflected the critical importance of self-efficacy, habit, and availability of resources in preventive behaviors.

In other words, building a truly resilient consumer against e-commerce fraud necessitates a multi-level approach, including practical skill development of the user; responsibility of the platform; and well-functioning and updated regulations. E-commerce platforms ought to offer readily identifiable, user-friendly safety functions; a transparent process of fraud complaint; and reliable and reasonable verification systems of sellers. Educational institutions and public entities shall focus not only on warning users but also on improving their capacity for spotting various forms of fraud. Regulators should continue to adapt laws that allow better response to digital frauds.

VIII. Future Research Direction

Future work could increase the sample size and geographic dispersion of study participants for enhanced generalization to diverse cultural and economic settings. Future work can investigate the prolonged change in digital literacy and fraud resistance by consumers after they gain more online experience. Further qualitative research into why fraud resistance behavior might still be inconsistent, even for digitally conscious customers, could offer rich insights into human behavior and vulnerability.

Research on how AI-powered tools could enhance consumers' digital literacy skills, or how platform design decisions influence how a customer combats fraud, also represents rich areas for further research.

REFERENCES

[1] Aloul, F., Zahidi, S., & Dutta, K. (2022). Enhancing online security through consumer awareness: A study on e-commerce fraud prevention. Journal of Cybersecurity, 8(2), 105–118.

[2] Bhangla, A., & Tuli, J. (2021). A study on cyber crime and its legal framework in India. International Journal of Law Management & Humanities, 4(2), 493–501.

[3] Boerman, S. C., Kruikemeier, S., & Borgesius, F. Z. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research, 48(7), 953–977.

[4] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. MIS Quarterly, 39(4), 837–864.

[5] Chawla, D., & Kumar, V. (2022). E-commerce and consumer protection in India: The emerging trend. Journal of Business Ethics, 176(3), 561–577.

[6] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474.

[7] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90.

[8] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125.

[9] Khan, M. A., Singh, R., & Sharma, P. (2021). Consumer behavior towards online fraud in emerging economies. Journal of Retailing and Consumer Services, 59, 102385.

[10] Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. International Review of Economics and Finance, 91, 364–377.

[11] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114.

[12] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology (pp. 153–176). Guilford Press.

[13] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382.

[14] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

[15] Wei, L., Peng, M., & Wu, W. (2021). Financial literacy and fraud detection: Evidence from China. International Review of Economics and Finance, 76, 478–494.