International Journal of Innovative Research in Management Studies (IJIRMS)
Volume 8, Issue 2, February 2026. pp.1-9.

THE IMPACT OF DIGITAL SCAM AWARENESS ON CONSUMER BEHAVIOUR IN ONLINE SHOPPING

S.Manjula[1], Dr.S.Krithiga Maheswari[2]

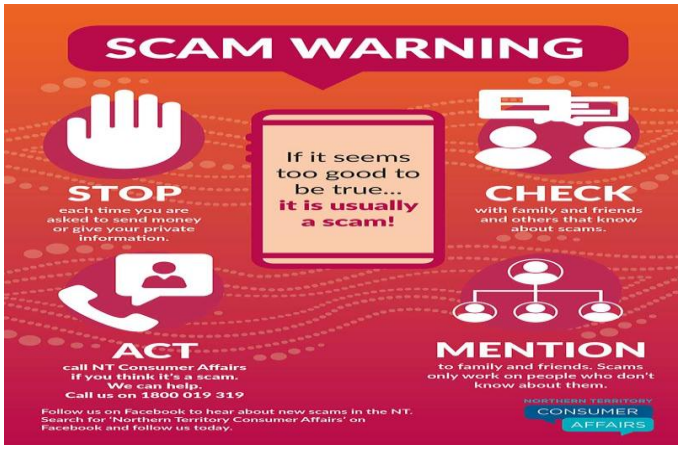
[1]*Research Scholar, PG and Research Department of Commerce (General), Shri Krishnaswamy College for Women, Anna Nagar, Chennai-40. Email ID: smadhan1231997@gmail.com*

[2]*Assistant Professor and Research Supervisor, PG and Research Department of Commerce (General), Shri Krishnaswamy College for Women, Anna Nagar, Chennai-40. Email- skcricketacademy@gmail.com*

Abstract—*The expansion of e-commerce and digital payment systems has significantly reshaped consumer purchasing patterns. While online shopping offers ease, speed, and wider access to products, it has also increased consumers' exposure to digital scams such as phishing, fake sellers, payment fraud, and identity theft. This study examines the extent of consumer awareness regarding digital scams and analyzes how such awareness influences online shopping behaviour. The research focuses on understanding how knowledge of online threats affects trust levels, purchasing frequency, platform selection, and adoption of secure payment practices. Data collected through a structured questionnaire highlights that consumers with higher scam awareness tend to be more cautious, selective, and security-conscious while shopping online. The findings emphasize the importance of digital literacy, robust security mechanisms, and consumer education in building confidence and safety within the digital marketplace.*

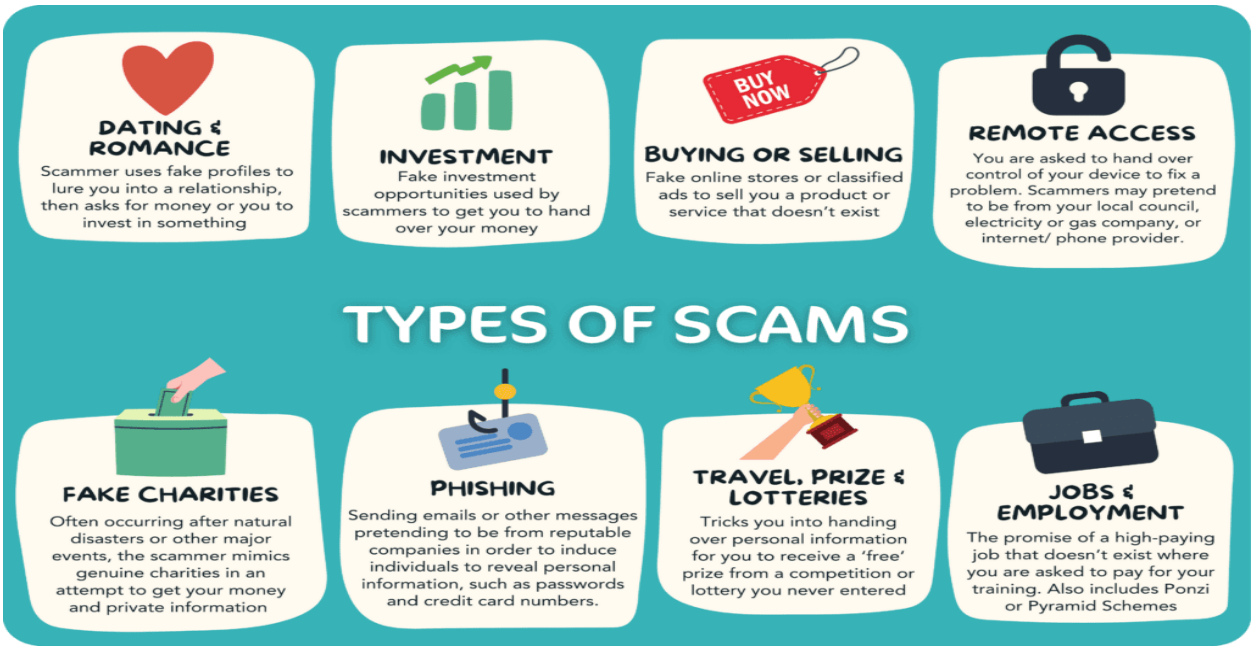
1. Introduction

In recent years, online shopping has become an essential component of modern consumer lifestyles, driven by advancements in internet technology and digital payment infrastructure. Consumers increasingly rely on e-commerce platforms for purchasing goods and services due to convenience, time efficiency, and competitive pricing. However, the growing dependence on digital platforms has simultaneously led to a rise in digital scams, posing serious risks to consumer trust and financial security.



Digital scams manifest in multiple forms, including phishing attacks, counterfeit websites, fraudulent sellers, payment manipulation, and misuse of personal information. Such fraudulent activities not only result in monetary loss but also weaken consumer confidence in online shopping environments. As awareness of these threats increases, consumers often adjust their behaviour by becoming more cautious, verifying sellers, and preferring secure payment options.

Consumer awareness plays a decisive role in shaping online shopping behaviour. Well-informed consumers are more likely to adopt protective measures, avoid suspicious platforms, and make rational purchasing decisions. Conversely, limited awareness increases vulnerability to scams and discourages digital participation. This study aims to analyze how awareness of digital scams influences online shopping behaviour and to identify strategies that can enhance consumer safety and confidence in e-commerce transactions.



10 Common Online Scams in India and How to Stay Protected

1. Phishing scams- Phishing scams use deceptive emails, text messages, or fake websites that impersonate trusted institutions such as banks or government bodies to steal confidential information like login credentials, bank details, or card numbers.

Example: An individual receives an email appearing to be from "XYZ Bank" stating that their account has a security issue. When they click the provided link, they are taken to a fraudulent website and unknowingly enter their banking details, which the scammer later exploits.

2. **OTP and UPI Scams -** In OTP and UPI frauds, scammers manipulate victims into revealing their one-time password or UPI PIN, enabling unauthorized financial transactions.

Example: A fraudster pretends to be a bank official and claims there is an urgent problem with the victim's account. By convincing the victim to share the OTP, the scammer completes a UPI transfer and withdraws money.

3. **Fake Job Offer -** Fake job scams target job seekers by offering non-existent employment opportunities and demanding fees for registration, processing, or security deposits.

Example: A candidate receives an email promising a high-paying job from a reputed company but is asked to pay ₹2,000 as a processing charge. After payment, all communication stops, revealing the offer was fraudulent

4. **Online** Shopping **Scam-**Online shopping scams involve counterfeit websites or fake social media pages advertising products at very low prices, but failing to deliver genuine goods or any product at all.

Example: A customer orders a smartphone from a seemingly genuine website offering heavy discounts. After making the payment, the product never arrives and the website disappears

5. Tech Support Scams-Tech support scams occur when fraudsters pose as customer support agents from well-known companies and claim there is a technical issue, gaining remote access to steal data or install malware. **Example:** A pop-up warning informs a user that their system is infected and urges them to contact "Microsoft Support." The scammer then accesses the computer remotely and steals personal information.

6. Loan Scams- Loan scams offer attractive loan schemes with minimal documentation but demand advance fees, after which no loan is provided.

Example: A person applies for an instant loan advertised online and pays a ₹3,000 processing fee. The lender disappears, and the loan is never sanctioned.

7. **Investment Scams and Ponzi Schemes-** These scams promise unrealistically high returns with little or no risk, often paying early investors using funds from new participants until the scheme collapses.

Example: A WhatsApp investment group assures quick double returns. Initial payouts build trust, but once larger investments are made, the group vanishes without a trace.

8. Fake Dating and Romance Scams-In romance scams, fraudsters create fake profiles on dating platforms, build emotional connections, and later request money under false pretenses.

Example: After weeks of online interaction, a scammer claims to need money for a medical emergency. Once the victim transfers funds, the profile disappears.

8. Loan App Scams and Digital Lending Fraud- Illegal lending apps provide quick loans but impose excessive interest rates, misuse personal data, and harass borrowers for repayment.

Example: A borrower takes a ₹5,000 loan through an app but is later pressured to repay ₹15,000 within days, along with threats and harassment.

9. Cryp to currency Investment Scams- Cryptocurrency scams attract investors with promises of massive profits, only to shut down platforms or block users after collecting funds.

Example: A Telegram group claims to offer fivefold returns within ten days. After investing, the platform becomes inaccessible and administrators disappear.

10. Ransomware Attacks - Ransomware is malicious software that locks or encrypts a victim's files, demanding payment—often in cryptocurrency—for restoring access.

Example: A small business suddenly loses access to all its data and receives a demand for ₹1 lakh in digital currency to recover the files.

2. LITERATURE REVIEW

2.1 Awareness of Online Security and Buying Decisions

Daud et al. (2020) found that increased awareness of cyber threats encourages consumers to adopt protective online behaviours. Their study revealed that although awareness improves caution, it may also reduce online shopping frequency due to heightened risk perception.

2.2 Consumer Trust and Online Purchase Hesitation

Nikhashem et al. (2011) identified transaction insecurity as a major barrier to online shopping. Even when consumers are aware of scams, inadequate practical knowledge leads to reduced trust and preference for offline shopping alternatives.

2.3 Protective Behaviour and Security Motivation

Hanus and Andy (2016), using Protection Motivation Theory, demonstrated that consumers with higher awareness of security threats are more likely to use secure payment methods and avoid unfamiliar websites, thereby altering their online shopping patterns.

2.4 Demographic Influence on Scam Awareness

Martens et al. (2019) highlighted that factors such as age, education, and technological familiarity significantly affect scam awareness and vulnerability. Younger and digitally literate consumers exhibit greater awareness and safer online behaviour.

2.5 Manipulative Digital Design and Consumer Perception

Brenncke (2024) examined how deceptive website designs and dark patterns influence consumer trust. Such practices negatively impact shopping confidence and reinforce cautious purchasing behaviour among aware consumer.

Objectives of the Study

- To measure the level of consumer awareness regarding various digital scams
- To examine the relationship between scam awareness and online shopping behaviour
- To identify factors influencing consumer trust in e-commerce platforms
- To suggest policy and platform-level improvements

Limitations of the Study

- The study is limited to **200 respondents**, which may restrict generalization.
- Convenience sampling was used, which may introduce sampling bias.
- The study is confined to selected geographic regions and time periods.
- Responses are based on self-reported data, which may involve bias.

3. RESEARCH METHODOLOGY

This chapter explains the research design, sampling procedure, data collection methods, tools used, and statistical techniques applied to analyze consumer awareness of digital scams and its influence on online shopping behaviour and trust in e-commerce platforms.

3.1 Research Design

The study adopts a **descriptive and analytical research design**.

- **Descriptive** design is used to assess the level of awareness regarding digital scams.
- **Analytical** design is used to examine relationships between scam awareness, online shopping behaviour, and consumer trust.

3.2 Data Collection Method

- The study is based on primary data, collected directly from consumers through a structured questionnaire.
- Secondary data were collected from journals, research articles, reports, and websites to support the theoretical framework.

3.3 Area of the Study

The study was conducted among **online shoppers** (urban consumers) who actively use e-commerce platforms.

3.4 Population of the Study

The population consists of **consumers who engage in online shopping and digital payment methods**.

3.5 Sample Size

A total of **200 respondents** were selected for the study.

3.6 Sampling Technique

The study uses the **Convenience Sampling Method**, as respondents were selected based on accessibility and willingness to participate.

3.7 Statistical Tools Used

Data were coded and analyzed using **SPSS software**.

Objective	Statistical Tool
Level of scam awareness	Percentage analysis, Mean, SD
Awareness vs demographics	One-Way ANOVA
Awareness & shopping behaviour	Chi-Square test
Relationship analysis	Pearson Correlation
Trust factor ranking	Weighted Mean
Influencing factors	Multiple Regression

4. DATA ANALYSIS AND INTERPRETATION

This chapter presents the analysis and interpretation of data collected from 200 respondents. The data were coded, tabulated, and analyzed using **SPSS**. Appropriate statistical tools such as percentage analysis, descriptive statistics, ANOVA, Chi-square test, correlation, weighted mean, and regression analysis were applied to test the objectives and hypotheses of the study.

4.2 Demographic Profile of Respondents

Table 4.1: Gender-wise Distribution

Gender	No. of Respondents	Percentage
Male	98	49.0
Female	102	51.0
Total	**200**	**100**

Interpretation:
The table shows that 51% of the respondents are female and 49% are male, indicating a nearly equal representation.

Table 4.2: Age-wise Distribution

Age Group	Respondents	Percentage
Below 20	32	16.0
21–30	78	39.0
31–40	54	27.0
Above 40	36	18.0
Total	**200**	**100**

Interpretation:
Most respondents (39%) belong to the age group of 21–30 years, showing high engagement in online shopping.

4.3 Level of Awareness Regarding Digital Scams (Objective 1)

Table 4.3: Descriptive Statistics – Awareness Level

Variable	Mean	Std. Deviation
Digital Scam Awareness	3.92	0.64

Interpretation:
The mean score of 3.92 indicates a **high level of awareness** regarding digital scams among consumers.

Table 4.4: ANOVA – Awareness vs Age Group

Source	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.62	3	1.87	4.32	0.005
Within Groups	84.78	196	0.43		
Total	**90.40**	**199**			

Interpretation:
Since the p-value (0.005) is less than 0.05, there is a **significant difference** in scam awareness across age groups. Hence, **H_0 is rejected**.

4.4 Relationship Between Scam Awareness and Online Shopping Behaviour (Objective 2)

Table 4.5: Chi-Square Test

Value	df	Asymp. Sig.
$\chi^2 = 12.45$	4	0.014

Interpretation:
As the p-value (0.014) is less than 0.05, there is a **significant association** between scam awareness and online shopping behaviour. Therefore, the null hypothesis is rejected.

Table 4.6: Pearson Correlation Analysis

Variables	Correlation (r)	Sig.
Awareness & Shopping Behaviour	0.62	0.000

Interpretation:
The positive correlation (r = 0.62) indicates that higher scam awareness leads to safer and more confident online shopping behaviour.

Table 4.8: Multiple Regression Analysis

Dependent Variable: Consumer Trust

Independent Variable	Beta	t-value	Sig.
Secure Payment	0.48	6.12	0.000
Customer Reviews	0.31	4.08	0.001
Return Policy	0.24	3.22	0.002
Brand Reputation	0.19	2.75	0.006

Model Summary:

- $R = 0.71$
- $R^2 = 0.50$

Interpretation:
The regression model explains **50% of the variance** in consumer trust. Secure payment systems have the strongest influence on trust.

4.6 Hypotheses Testing Summary

Hypothesis	Test	Result
H_{01}	ANOVA	Rejected
H_{02}	Chi-Square	Rejected
H_{03}	Regression	Rejected

FINDINGS, SUGGESTIONS AND CONCLUSION

5.1 Introduction

This chapter presents the key findings derived from the statistical analysis of primary data collected from 200 respondents. The findings are directly aligned with the objectives of the study and are supported by results obtained through SPSS. Based on these findings, appropriate suggestions are offered, followed by the conclusion of the study.

5.2 Major Findings of the Study

Findings Related to Objective 1

To measure the level of consumer awareness regarding various digital scams

- The overall mean score of **3.92** indicates that consumers possess a **high level of awareness** regarding digital scams.
- Respondents demonstrate greater awareness of **phishing emails, fake e-commerce websites, and OTP-related frauds** compared to other forms of digital scams.
- The results of **One-Way ANOVA** reveal a **statistically significant difference** in awareness levels across different age groups, indicating that **demographic factors influence consumer awareness** of digital scams.

Findings Related to Objective 2

To examine the relationship between scam awareness and online shopping behaviour

- The **Chi-square test** confirms a **significant association** between digital scam awareness and online shopping behaviour.
- **Pearson correlation analysis** shows a **strong and positive relationship (r = 0.62)** between scam awareness and safe online shopping behaviour.
- Consumers with higher awareness levels are more likely to **verify seller authenticity, avoid suspicious links, and adopt safer purchasing practices**.

Findings Related to Objective 3

To identify factors influencing consumer trust in e-commerce platforms

- **Secure payment systems** are identified as the **most influential factor** affecting consumer trust in e-commerce platforms.
- **Customer reviews and transparent return and refund policies** significantly contribute to enhancing consumer trust.
- **Multiple regression analysis** indicates that security-related features have the **strongest impact on consumer trust** compared to other factors.
- The regression model explains **50 percent of the variation** in consumer trust, suggesting a **good model fit**.

5.3 Suggestions of the Study

5.3.1 Policy-Level Suggestions

- Government agencies should organize **regular digital literacy and cyber safety awareness programs** to educate consumers about emerging digital scams.
- **Cybercrime reporting systems** should be simplified and made more accessible to encourage timely reporting of online fraud.
- Stronger **legal and regulatory frameworks** should be enforced to deter cybercriminal activities and protect consumer interests.

5.3.2 Platform-Level Suggestions

- E-commerce platforms should adopt **AI-based fraud detection and monitoring systems** to identify suspicious activities in real time.
- **Mandatory seller verification** and periodic platform audits should be implemented to prevent fraudulent sellers.
- Platforms should ensure **clear communication of return, refund, and grievance redressal policies**.
- **In-app alerts and security notifications** should be provided to warn users about potential scams

5.3.3 Consumer-Level Suggestions

- Consumers should carefully **verify website URLs and seller credentials** before making purchases.
- **Two-factor authentication** should be enabled for all online transactions.
- Consumers should regularly update their knowledge of **cyber safety guidelines and best practices**.

5.5 Scope for Future Research

- Future studies may include a **larger and more diverse sample** to improve generalizability.
- Comparative research can be conducted between **urban and rural consumers** or across different regions.
- Longitudinal studies may examine **changes in digital scam awareness over time**.
- Advanced statistical techniques such as **Structural Equation Modeling (SEM)** may be employed for deeper analysis.

5.6 Conclusion

The study concludes that consumers exhibit a **high level of awareness regarding digital scams**, which significantly influences their online shopping behaviour. Secure payment systems, customer reviews, and transparent platform policies play a crucial role in building consumer trust in e-commerce platforms. Strengthening digital literacy initiatives and enhancing platform security measures are essential to safeguard consumers and support the sustainable growth of the e-commerce ecosystem.

REFERENCES

[1] Brenncke, M. (2024). Dark patterns and deceptive design in digital marketplaces: Implications for consumer trust and decision-making.

[2] Daud, N. M., Ab Hamid, N., & Wan Abdullah, W. M. (2020). Consumer awareness of cyber security threats and its impact on online purchasing behaviour.

[3] Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on online purchase intention: Protection Motivation Theory perspective.

[4] Martens, Y., De Wolf, R., & Vanden Abeele, M. (2019). Vulnerability and digital scam awareness: The role of age, education, and digital literacy.

[5] Nikhashem, S. R., Paim, L., Osman, S., & Sidin, S. M. (2011). Transaction insecurity and online shopping hesitation: A consumer trust perspective.

[6] Reserve Bank of India. *(2023).* Digital payment security and fraud prevention measures. RBI Bulletin.

[7] National Cyber Crime Reporting Portal. (2024). *Types* of cyber crimes *and* preventive measures. Government of India.

[8] OECD. (*2022).* Consumer policy and fraud in the digital age. Organisation for Economic Co-operation and Development.

[9] Verma, M., & Arora, R. (2021). Online frauds and consumer protection in India: An empirical study.

[10] Kumar, V., & Ayodeji, O. (2020). E-commerce security, trust, and consumer behaviour: A systematic review.

[11] Awanis, S., & Cui, C. C. (2014)."Consumer susceptibility to scams and online shopping behavior.

[12] Jansen, J., & van Schaik, P. (2020). "The impact of fear of online fraud on consumers' online shopping behavior.

[13] Li, Y., & Zhang, R. (2021). "How phishing awareness training influences online shopping decisions."

[14] FTC (Federal Trade Commission). (2023). "Consumer Sentinel Network Data Book 2022

*****