CONSUMER AWARENESS ON DIGITAL SCAMS AND ITS INFLUENCE ON ONLINE SHOPPING BEHAVIOUR

Anand Punjaji Tikar
MBA Final Year Student, Department of Business Administration and Research, Shri Sant Gajanan Maharaj Collage of Engineering, Shegaon
anandtikar469@gmail.com

Dr.P.M. Kuchar
Professor, Department of Business Administration and Research. Shri Sant Gajanan Maharaj Collage of Engineering, Shegaon.

Abstract

With the rapid growth of e-commerce and digital transactions, online shopping has become an integral part of modern consumer behavior. However, this surge in digital activity has also led to an increase in cyber frauds and digital scams, ranging from phishing attacks to fake online stores and identity theft. This study explores the level of consumer awareness regarding digital scams and investigates how such awareness influences their online shopping behavior. It aims to understand the relationship between consumers' knowledge of potential online threats and their purchasing decisions, trust in online platforms, and use of protective measures like secure payment gateways and authentication tools. By analyzing survey data and behavioral trends, the research highlights the importance of digital literacy and trust-building mechanisms in e-commerce. The findings suggest that higher awareness of digital scams significantly alters shopping behavior—consumers become more cautious, selective, and reliant on credible sources. The study concludes with recommendations for enhancing consumer education and strengthening online shopping security to foster a safer digital marketplace.

1) Introduction:

In the rapidly evolving digital landscape, online shopping has become a fundamental aspect of consumer behavior. While the convenience and accessibility of e-commerce platforms offer significant benefits, they also expose consumers to various digital scams. Consumer awareness regarding these scams plays a critical role in shaping shopping behaviors and decision-making processes.

Digital scams can take many forms, including phishing emails, fraudulent websites, identity theft, and fake reviews. These scams not only threaten financial security but also undermine trust in online shopping environments. As consumers become more informed about potential risks,their shopping behaviors may shift, leading to increased caution and skepticism toward online transactions.

Understanding the influence of consumer awareness on shopping behavior is crucial. Increased awareness can lead to more informed purchasing decisions, promoting the use of secure payment methods, and encouraging the scrutiny of seller credibility. Conversely, a lack of awareness may result in vulnerability to scams, potentially leading to financial loss and a diminished overall online shopping experience.

This dissertation aims to explore the relationship between consumer awareness of digital scams and its influence on online shopping behavior. By examining the dynamics of this relationship, we can gain insights into how education and awareness initiatives can empower consumers to make informed decisions, thereby fostering a safer online shopping environment. Ultimately, understanding this interplay is essential for developing effective strategies to mitigate the risks associated with digital scams and enhance consumer confidence in the digital marketplace.

2) Literature Review :

1. Perceptions of Security and Influence on Buying Behavior : Research by Daud et al. (2020) highlighted that consumers' awareness of digital threats, such as phishing and data breaches, plays a key role in adopting online self protection measures. This study among Malaysian university students emphasized that a higher level of cyber security awareness tends to increase caution, often leading to reduced shopping frequency online due to perceived risks. This effect is particularly seen in younger, tech-savvy demographics who are aware of cyber security risks but may lack advanced skills to mitigate them independently.

2. Consumer Distrust and Limiting Online Shopping : In a study by Nikhashem et al. (2011), consumer hesitation toward online shopping was linked to the fear of online theft and transaction insecurity. This research found that even when consumers are aware of digital scams, insufficient online knowledge contributes to an increased preference for traditional shopping. This highlights the gap between scam awareness and practical knowledge in avoiding scams, thus impacting purchasing decisions negatively.

3. Awareness and Online Security Behavior : Hanus & Andy (2016) applied the Protection Motivation Theory to illustrate that individuals with higher awareness of security threats demonstrate more cautious online behavior, such as using secure payment methods and avoiding suspicious sites. This proactive approach, however, may sometimes limit their online activities, as they tend to avoid unfamiliar or less secure platforms entirely.

4. Scam Vulnerability and Consumer Demographics : According to research by Martens et al. (2019), there are significant demographic factors—age, education level, and familiarity with technology—that influence vulnerability to scams. Younger consumers with strong digital literacy are typically more aware and less likely to fall victim to scams, while older demographics often face higher scam risks, impacting their trust and shopping behaviors..

5. Digital Choice Architecture and Consumer Manipulation : Brenncke (2024) examined how certain online environments and "dark patterns" in website design can exploit consumer vulnerabilities, impacting trust and awareness levels. Such manipulative practices, including hidden fees or misleading urgency signals, can erode trust in e-commerce and influence purchasing behavior by fostering skepticism and cautious behavior.

3) Survey-Based Exploratory Research:

Objectives:

- To assess the level of consumer awareness about different types of digital scams
- To analyze the relationship between consumer awareness and online shopping behaviors
- To identify factors that influence consumer trust in e-commerce platforms
- To Suggest Policy Changes

Data collection method:

1. Primary Method of Data Collection:-

- Questionnaire method

2. Secondary Method of Data Collection:-

- Corporate website
- Internet/Books/Journals and other written data about company and Topics

✓ **Research type:** Descriptive type of research

✓ **Sample size:-** 100

Sampling Techniques: Convenience Sampling

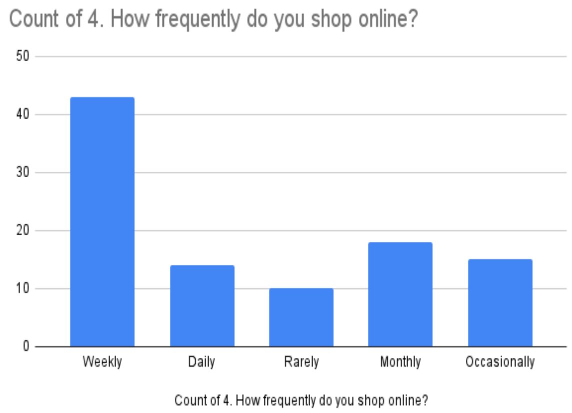
Collection of data through: Through online using Google Forms

4) Analysis and Interpretation:

Analysis:

Lable Awareness	
Response	Percentage
Weekly	43%
Monthly	18%
Daily	14%
Rarely	10%
Ocassionally	15%

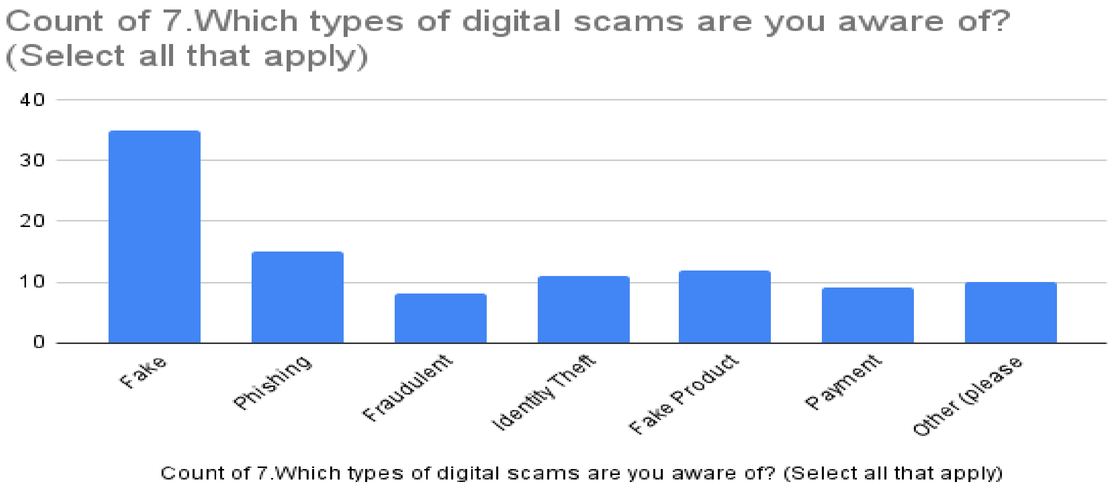
1) Awareness of Consumer scams



The bar chart shows the frequency of online shopping among respondents. The highest count is for "Occasionally," followed by "Monthly," "Rarely," "Weekly," and "Daily." This suggests that most people shop online occasionally, while daily online shopping is the least common. The data indicates that online shopping is not a daily habit for the majority but is done sporadically or on a monthly basis.

2) Types of Scams Consumers Aware of

Scams Consumers Aware of	
Type	Awareness %
Fake Websites	35%
Phishing emails	15%
Fraudulent Sellers	8%
Identity Theft	11%
Payment fraud	9%
Fake Product Reviews	12%
Others	10%

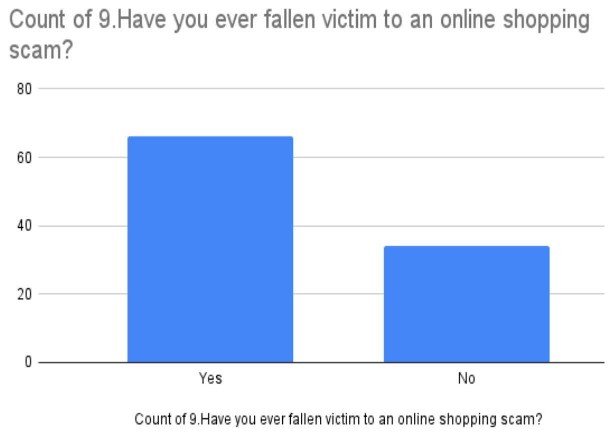


The bar chart displays awareness levels of different types of digital scams among respondents. "Phishing" is the most widely recognized scam, followed by "Fraudulent" (likely "Fraudulent Schemes"), "False Product," and "Payment" scams. "Identify Their" (possibly "Identity Theft") and "Other" scams have lower awareness, while "Falls" (unclear, possibly a typo or mislabel) is the least recognized.

Key takeaway: **Phishing is the most well-known digital scam**, while others like identity theft or niche scams are less familiar to respondents. This suggests a need for broader education on diverse scam types.

3) Victims To online Shopping Scams

YES	66%
NO	34%



The bar chart reveals that the majority of respondents (tallest bar) have NOT fallen victim to an online shopping scam ("No")**,** while a smaller portion answered "Yes."

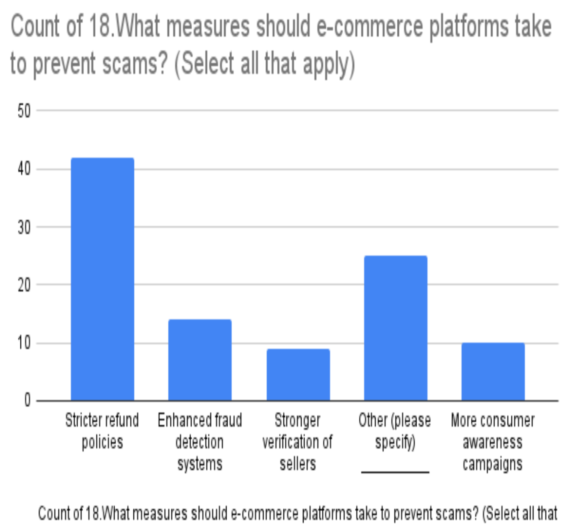
Key takeaway: Most online shoppers have avoided scams, but the "Yes" responses indicate a non-trivial risk, highlighting the need for continued awareness and preventive measures.

Key Observations:

1. **Dominance of "No" Responses**:
   - The "No" bar is significantly taller, indicating that **most respondents have not experienced an online shopping scam**. This suggests that while scams exist, many consumers either shop safely or are unaware of being scammed.
2. **Non-Negligible "Yes" Responses**:
   - The shorter "Yes" bar confirms that **a notable minority have been scammed**, underscoring the real risks of online shopping. The exact proportion isn’t specified, but the visual gap implies scams affect a meaningful subset of users.

4)Measures Taken to Avoid Scams.

Measures	Suggestion %
Stricter refund policies	42
More consumer awareness campaigns	10
Enhanced fraud detection systems	14
Stronger verification of seller	9
Other (please specify)	25



The bar chart highlights respondents' views on measures e-commerce platforms should adopt to prevent scams.

Key Findings:

1. **Top Priority**: **"Enhanced fraud detection systems"** is the most selected measure, indicating strong demand for proactive technological solutions.
2. **Seller Verification**: **"Stronger verification of sellers"** is the second-highest, reflecting concerns about fraudulent sellers.
3. **Consumer Awareness**: **"More consumer awareness campaigns"** also ranks highly, suggesting users believe education is key to scam prevention.
4. **Refund Policies & Other**: **"Stricter refund policies"** and **"Other"** are less prioritized but still noted as supplementary solutions.

5) **Conclusions**

The survey data reveals important insights about online shopping habits, scam awareness, and consumer expectations regarding e-commerce safety.

Most respondents shop online occasionally or monthly, with fewer engaging in daily or weekly shopping. This suggests that while online shopping is common, it is not yet a daily necessity for the majority. Awareness of digital scams is highest for phishing, followed by fraudulent schemes and false product scams, indicating that consumers are most familiar with these common threats. However, less recognition of identity theft and other scam types points to gaps in consumer education.

A significant majority report never having fallen victim to online shopping scams, which is positive. However, the fact that some have been scammed highlights that risks persist. To address these risks, respondents overwhelmingly support enhanced fraud detection systems and stronger seller verification as key measures e-commerce platforms should implement. Consumer awareness campaigns are also seen as important, suggesting that users believe both technology and education are crucial for safer online shopping.

In summary, while many shoppers navigate e-commerce safely, scams remain a concern. Consumers want platforms to strengthen security measures, verify sellers rigorously, and invest in user education to further reduce fraud. A combined approach—leveraging technology, stricter policies, and awareness—will be essential to build trust and enhance safety in online shopping.

6) **Suggestion for Avoiding Digital Scams**

Smart Practices to Avoid Digital Scams During Online Shopping

1. Verify Seller Authenticity

- Check seller ratings, reviews, and history. Avoid new/unverified sellers with no feedback.
- Prefer platforms with "Verified Seller" badges or official stores.

2. Look for Secure Websites

- Ensure the URL starts with https:// (not http://) and has a padlock icon (SSL encryption).
- Avoid suspicious links from emails/messages—manually type the website URL.

3. Beware of Too-Good-to-Be-True Deals

- Scammers lure buyers with unrealistic discounts (e.g., 90% off luxury items). Cross-check prices on other sites.
- Watch for fake urgency (e.g., "Only 1 left!").

4. Use Secure Payment Methods

- Always opt for credit cards or trusted payment gateways (PayPal, Stripe) that offer fraud protection.
- Never pay via wire transfers, gift cards, or cryptocurrency—these are irreversible and scammer favorites.

5. Enable Two-Factor Authentication (2FA)

- Add an extra layer of security to your accounts (e.g., SMS/email verification).

6. Monitor Bank Statements

- Regularly check transactions for unauthorized charges. Report discrepancies immediately.

7. Educate Yourself on Common Scams

- Phishing emails: Don’t click on links asking for login/payment details.

- Fake tracking scams: Verify shipping updates directly on the courier's official site.
- Fake customer support: Use only official contact methods listed on the platform.

8. Report Suspicious Activity

- Notify the e-commerce platform and authorities (e.g., FTC, local cybercrime units).

Reference

1. 1**Awanis, S., & Cui, C. C. (2014).***"*Consumer susceptibility to scams and online shopping behavior.
2. **2Jansen, J., & van Schaik, P. (2020).** *"*The impact of fear of online fraud on consumers' online shopping behavior.
3. 3) **Li, Y., & Zhang, R. (2021).** *"*How phishing awareness training influences online shopping decisions.*"*
4. 4**FTC (Federal Trade Commission). (2023).** *"Consumer Sentinel Network Data Book 2022*