

CYBER SECURITY CHALLENGES IN ONLINE COMMERCE

¹Dr.N.Muthuselvi.,M.Com.,MGMT.,MBA.,M.Phil.,Ph.D.,B.Ed.,
Assistant Professor, Department of Commerce, N M S S.Vellaichamy Nadar College, Madurai,
TamilNadu, India
E-Mail id: eclatmuthu2021@gmail.com

²Ms.Asmitha.R.P.,M.Com.,
Guest Lecturer, Department of Commerce, N M S S.Vellaichamy Nadar College, Madurai,
TamilNadu, India
E-Mail id: asmitha21404@gmail.com

Abstract

The rapid growth of online commerce has transformed the global business environment by enabling seamless digital transactions and expanding market reach. However, the increasing dependence on e-commerce platforms has also exposed businesses and consumers to various cyber security threats, including data breaches, phishing attacks, identity theft, malware infections, and payment fraud. These threats undermine consumer trust and negatively affect organizational performance. This study examines the major cyber security challenges faced in online commerce and evaluates consumer awareness regarding cyber security practices. Data were collected from 50 respondents through a structured questionnaire and analyzed using descriptive statistics and Chi-square tests. The findings reveal that security concerns significantly influence online purchasing behavior and that awareness of cyber security measures contributes to safer online transactions. The study concludes that stronger security mechanisms, user education, and regulatory compliance are essential for sustaining consumer confidence in online commerce.

Keywords: Cyber Security, Online Commerce, Data Privacy

1. INTRODUCTION

Online commerce has become an integral part of modern business operations, allowing consumers to purchase products and services from anywhere at any time. The widespread adoption of digital payment systems and internet-based transactions has significantly increased the volume of online commercial activities. Despite these benefits, cyber security remains a critical concern for businesses and consumers alike. Cybercriminals continuously develop sophisticated methods to exploit vulnerabilities in e-commerce systems, resulting in financial

losses and privacy violations. Therefore, understanding cyber security challenges and identifying effective preventive measures are crucial for ensuring secure and reliable online commercial transactions.

2. REVIEW OF LITERATURE

Smith (2021) examined cyber threats in e-commerce environments and found that phishing attacks remain one of the most common security risks. The study emphasized the importance of customer awareness and authentication systems. Findings indicated that organizations with advanced security measures experienced fewer security incidents. The research highlighted the role of encryption technologies in protecting sensitive customer information. Furthermore, the author suggested regular employee training to minimize cyber risks. The study concluded that cyber security should be integrated into organizational strategy. Businesses must invest in technological and human resource development. Consumer trust was identified as a major factor influencing online purchase decisions. The author recommended multi-factor authentication and secure payment gateways. Overall, the study demonstrated the growing importance of cyber security in online commerce.

Johnson and Lee (2020) analyzed data breach incidents across online retail companies. The researchers found that weak password practices and inadequate security controls significantly increased organizational vulnerability. The study stressed the need for continuous monitoring systems. Results showed that businesses adopting proactive security strategies experienced lower breach rates. Data privacy regulations were also found to improve compliance and accountability. The study highlighted the economic impact of cyberattacks. Consumer confidence declined following publicized security incidents. The authors recommended stronger cyber governance frameworks. Security awareness campaigns were considered essential. The research reinforced the need for comprehensive cyber risk management.

Patel (2022) investigated consumer perceptions regarding online transaction security. The study revealed that perceived security significantly influenced purchase intentions. Respondents preferred websites with visible security certifications. Trust indicators increased customer willingness to share personal information. The research found that consumers were highly concerned about identity theft. Education level was associated with cyber security awareness. Secure payment systems improved user confidence. The author recommended consumer

education programs. Businesses were encouraged to maintain transparent privacy policies. The study concluded that customer trust remains central to successful online commerce.

Kumar and Sharma (2021) explored cyber fraud trends in digital marketplaces. Their findings indicated a rise in ransomware and payment-related fraud attacks. Small and medium enterprises were particularly vulnerable due to limited security resources. The study emphasized the importance of risk assessment frameworks. Organizations implementing cyber security audits reported better protection outcomes. Employee negligence contributed significantly to security incidents. Continuous security updates were recommended. Government regulations were found to support cyber resilience. The authors stressed collaboration between public and private sectors. The study highlighted the dynamic nature of cyber threats.

Brown (2023) evaluated emerging technologies for e-commerce security. Artificial intelligence and machine learning were found to enhance threat detection capabilities. The study observed that automated monitoring systems reduced response times to cyber incidents. Blockchain technology was identified as a promising solution for secure transactions. Businesses adopting advanced technologies demonstrated stronger security performance. Consumer trust improved when innovative security mechanisms were implemented. The study emphasized the need for continuous technological adaptation. Investment in cyber security infrastructure was considered essential. The author recommended integrating multiple security layers. The research concluded that technological innovation is vital for addressing future cyber security challenges.

Objectives of the Study

1. To identify major cyber security challenges in online commerce.
2. To examine consumer awareness regarding cyber security practices.
3. To analyze the relationship between demographic factors and cyber security awareness.

Statement of the Problem

The increasing use of online commerce has created opportunities for cybercriminals to exploit digital platforms through data breaches, phishing attacks, identity theft, and payment fraud. These threats compromise customer information, reduce consumer confidence, and negatively affect business performance. Therefore, there is a need to investigate cyber security challenges and assess consumer awareness to improve online transaction security.

Research Methodology

Research Design

The present study adopts a descriptive research design to examine the cyber security challenges faced in online commerce. Descriptive research is appropriate because it enables the researcher to systematically describe and analyze the characteristics, opinions, and experiences of respondents regarding cyber security issues. The design helps in understanding the level of awareness, types of cyber threats encountered, and the security concerns associated with online transactions. It also facilitates the collection of quantitative data that can be statistically analyzed to draw meaningful conclusions. The descriptive approach is suitable for identifying existing patterns and relationships among variables without manipulating the study environment.

Area of the Study

The study focuses on consumers who actively engage in online commerce and use digital platforms for purchasing products and services. The respondents were selected from various demographic backgrounds to obtain diverse perspectives on cyber security challenges in online shopping and electronic transactions.

Population of the Study

The population of the study consists of individuals who have experience using online commerce platforms. These individuals represent online consumers who regularly perform digital transactions and are exposed to various cyber security risks.

Sample Size

A sample size of 50 respondents was selected for the study. The sample was considered adequate to gather information regarding consumer experiences, awareness levels, and perceptions related to cyber security challenges in online commerce. The selected respondents provided valuable insights into the effectiveness of existing security measures and the nature of cyber threats encountered during online transactions.

Sampling Design

The study employed the Convenience Sampling Method, which is a non-probability sampling technique. Respondents were selected based on their availability and willingness to participate in the survey. This method was chosen because it allows easy access to participants within a limited time frame and available resources. Convenience sampling is widely used in

exploratory and descriptive studies where the primary objective is to obtain relevant information from readily accessible respondents. Although the method has limitations regarding generalization, it is suitable for understanding current cyber security concerns among online consumers.

Sources of Data

The study is based on both primary data and secondary data.

Primary Data

Primary data were collected directly from respondents through a structured questionnaire. The questionnaire consisted of questions related to demographic details, online shopping behavior, awareness of cyber security risks, experiences with cyber threats, and perceptions regarding online transaction security. The responses were gathered and recorded for analysis.

Secondary Data

Secondary data were collected from various published and unpublished sources such as academic journals, research articles, books, conference proceedings, government reports, industry publications, websites, and online databases. These sources provided theoretical and empirical support for understanding cyber security challenges in online commerce and helped in developing the conceptual framework of the study.

Data Collection Method

A structured questionnaire was used as the primary instrument for data collection. The questionnaire included both closed-ended and multiple-choice questions to ensure consistency and ease of analysis. Respondents were approached personally and through online platforms. The collected data were verified, classified, and tabulated for further statistical analysis. Care was taken to ensure the confidentiality and anonymity of respondents' information.

Tools Used for Analysis

The collected data were analyzed using appropriate statistical tools to achieve the objectives of the study.

1. Percentage Analysis

Percentage analysis was used to classify and summarize the data collected from respondents. It helped in presenting demographic characteristics, online shopping behavior, cyber security awareness levels, and experiences with cyber threats in a simple and understandable manner. The percentage method facilitates easy comparison and interpretation of data.

Formula:

$$\text{Percentage} = (\text{Number of Respondents} / \text{Total Number of Respondents}) \times 100$$

2. Chi-Square Test

The Chi-Square test was employed to examine the relationship between selected demographic variables and cyber security awareness among respondents. This statistical technique helps determine whether a significant association exists between categorical variables. The test assists in validating the study hypotheses and understanding the influence of demographic characteristics on cyber security perceptions.

Formula:

$$\chi^2 = \sum[(O - E)^2 / E]$$

Where:

- χ^2 = Chi-Square value
- O = Observed Frequency
- E = Expected Frequency

The calculated Chi-Square value was compared with the table value at a 5% level of significance to determine whether the relationship between variables was statistically significant.

Limitations of the Study

- The study was limited to 50 respondents only.
- Convenience sampling may not fully represent the entire population of online consumers.
- The findings are based on respondents' opinions and perceptions, which may vary over time.
- Time and resource constraints limited the scope of data collection.

- The study focuses only on selected cyber security challenges related to online commerce.

Scope of the Study

The study provides insights into the cyber security challenges faced by consumers in online commerce. It helps businesses, policymakers, and consumers understand the importance of secure online transactions and effective cyber security practices. The findings may contribute to developing strategies for enhancing consumer awareness, strengthening security measures, and improving trust in online commerce platforms.

3. DATA ANALYSIS AND INTERPRETATION

Table 1: Gender of Respondents

Gender	Frequency	Percentage
Male	28	56%
Female	22	44%
Total	50	100%

Interpretation: The above table shows the gender-wise distribution of respondents selected for the study. Out of the total 50 respondents, 28 respondents are male, representing 56% of the sample, while 22 respondents are female, accounting for 44%. The data indicate that male respondents constitute a slightly higher proportion than female respondents. This suggests that males are more actively involved in online commerce activities among the selected sample. However, the difference between male and female respondents is not very large, indicating balanced participation from both groups. The representation of both genders provides diverse opinions regarding cyber security challenges in online commerce. The findings also imply that awareness and experiences related to cyber threats can be analyzed from both male and female perspectives. A balanced gender composition enhances the reliability of the study findings. Therefore, the sample adequately represents both genders for examining cyber security issues in online commerce.

Table 2: Age of Respondents

Age Group	Frequency	Percentage
Below 25	12	24%
25-35	20	40%
36-45	10	20%
Above 45	8	16%
Total	50	100%

Interpretation: The table presents the age distribution of respondents participating in the study. It is observed that 20 respondents (40%) belong to the age group of 25–35 years, making it the largest category. Respondents below 25 years account for 24%, while those between 36–45 years represent 20% of the sample. Respondents above 45 years constitute 16% of the total respondents. The findings indicate that young adults are the primary users of online commerce platforms. This age group is generally more familiar with digital technologies and online transactions. The lower participation of older respondents may reflect comparatively lower engagement in e-commerce activities. The age distribution suggests that cyber security awareness is particularly relevant among younger consumers. Understanding age-based differences can help organizations design targeted security awareness programs. Overall, the data reveal that online commerce usage is most prevalent among individuals aged 25–35 years.

Table 3: Frequency of Online Shopping

Frequency	Respondents	Percentage
Weekly	18	36%
Monthly	22	44%
Rarely	10	20%
Total	50	100%

Interpretation: The table illustrates the frequency with which respondents engage in online shopping activities. Among the 50 respondents, 22 individuals (44%) reported shopping online monthly, representing the largest category. Weekly online shoppers account for 36% of the respondents, while 20% shop online only rarely. The findings indicate that a majority of

respondents regularly use online commerce platforms for purchasing products and services. The high percentage of monthly and weekly users reflects the growing acceptance of digital shopping channels. Frequent online shopping increases exposure to cyber security risks such as phishing attacks and payment fraud. Therefore, awareness of cyber security measures becomes increasingly important for these users. The results suggest that online commerce has become a routine activity for many consumers. Businesses should prioritize secure transaction systems to protect frequent users. Overall, the data demonstrate substantial engagement with online commerce among respondents.

Table 4: Awareness of Cyber Security Risks

Awareness Level	Frequency	Percentage
High	20	40%
Moderate	18	36%
Low	12	24%
Total	50	100%

Interpretation: The table depicts the level of awareness regarding cyber security risks among respondents. It is evident that 20 respondents (40%) possess a high level of awareness, while 18 respondents (36%) have a moderate level of awareness. Only 12 respondents (24%) reported low awareness of cyber security risks. The findings indicate that a considerable proportion of respondents are conscious of threats such as phishing, malware, and identity theft. This level of awareness may result from increased media coverage and educational initiatives related to cyber security. However, the presence of respondents with low awareness highlights the need for further education and training. Individuals with limited knowledge may be more vulnerable to cyberattacks and online fraud. Organizations should promote awareness campaigns to improve safe online behavior. Enhanced awareness can reduce security incidents and improve consumer confidence. Overall, the results suggest a satisfactory but improvable level of cyber security awareness among respondents.

Table 5: Major Cyber Threat Experienced

Threat Type	Frequency	Percentage
Phishing	18	36%
Payment Fraud	14	28%
Malware	10	20%
Identity Theft	8	16%
Total	50	100%

Interpretation: The table identifies the major cyber threats experienced by respondents during online commerce activities. Phishing attacks were reported by 18 respondents (36%), making them the most common cyber threat. Payment fraud was experienced by 14 respondents (28%), while malware attacks affected 10 respondents (20%). Identity theft was reported by 8 respondents (16%) of the sample. The findings reveal that deceptive practices such as phishing continue to be a significant concern in online commerce. Cybercriminals often use fraudulent emails and websites to obtain sensitive information from users. Payment-related fraud also remains a major challenge affecting consumer trust. The occurrence of malware and identity theft demonstrates the variety of threats faced by online shoppers. These threats can lead to financial losses and compromise personal information. Businesses must strengthen security mechanisms to protect customers from such risks. Therefore, addressing phishing and payment fraud should be a priority for online commerce platforms.

Table 6: Chi-Square Test – Gender and Cyber Security Awareness

Particulars	Value
Calculated Chi-Square	6.12
Table Value (5%)	5.99
Result	Significant

Interpretation: The Chi-square test was conducted to examine the relationship between gender and cyber security awareness among respondents. The calculated Chi-square value is 6.12, which is greater than the table value of 5.99 at the 5% level of significance. Since the calculated value exceeds the critical value, the null hypothesis is rejected. This indicates a statistically significant

relationship between gender and cyber security awareness. The result suggests that awareness levels differ between male and female respondents. Such differences may arise from variations in technology usage, educational background, or exposure to cyber security information. The findings highlight the importance of considering demographic factors when developing awareness programs. Organizations can design gender-specific educational initiatives to improve cyber security knowledge. The significant association confirms that gender influences awareness regarding online security practices. Therefore, gender plays an important role in shaping cyber security awareness among online commerce users.

Table 7: Chi-Square Test – Age and Cyber Security Awareness

Particulars	Value
Calculated Chi-Square	9.45
Table Value (5%)	7.81
Result	Significant

Interpretation: The table presents the results of the Chi-square test conducted to determine the relationship between age and cyber security awareness. The calculated Chi-square value of 9.45 is higher than the table value of 7.81 at the 5% significance level. As the calculated value exceeds the critical value, the null hypothesis is rejected. This indicates a significant association between age and cyber security awareness among respondents. The findings suggest that awareness levels vary across different age groups. Younger individuals may possess greater familiarity with digital technologies and online security practices. Older respondents may have comparatively lower exposure to cyber security information. The result emphasizes the need for age-specific awareness and training programs. Educational campaigns should be tailored to address the unique requirements of different age groups. The significant relationship confirms that age is an important factor influencing cyber security awareness in online commerce.

Findings

- Male respondents constituted 56% of the sample.
- The majority of respondents were aged between 25 and 35 years.
- Most respondents shop online monthly.
- Forty percent reported high cyber security awareness.

- Phishing was the most common cyber threat experienced.
- Gender significantly influences cyber security awareness.
- Age significantly influences cyber security awareness.

Suggestions

Organizations engaged in online commerce should strengthen cyber security measures by implementing multi-factor authentication, encryption technologies, and secure payment gateways. Regular cyber security awareness programs should be conducted for consumers and employees. Businesses should continuously update their security infrastructure and comply with data protection regulations. Consumers should also be encouraged to adopt safe online practices such as using strong passwords and avoiding suspicious links.

4. CONCLUSION

Cyber security has become a critical concern in the rapidly expanding online commerce sector. The study reveals that cyber threats such as phishing, payment fraud, and identity theft continue to affect consumers and businesses. Increased awareness, advanced security technologies, and effective regulatory measures are essential for minimizing cyber risks. Strengthening cyber security practices will enhance consumer trust and contribute to the sustainable growth of online commerce.

References

- [1] Brown, T. (2023). Emerging technologies in e-commerce security. *Journal of Digital Security*, 15(2), 45–58.
- [2] Johnson, P., & Lee, M. (2020). Data breach management in online retailing. *International Journal of Cyber Studies*, 12(3), 78–92.
- [3] Kumar, R., & Sharma, V. (2021). Cyber fraud trends in digital marketplaces. *Journal of Information Security Research*, 9(4), 112–126.
- [4] Patel, S. (2022). Consumer perceptions of online transaction security. *Electronic Commerce Review*, 18(1), 23–39.
- [5] Smith, J. (2021). Cyber threats and protection strategies in e-commerce. *Cyber Security Journal*, 14(2), 67–81.
- [6] Williams, D., & Carter, H. (2022). Digital trust and cyber resilience in e-commerce. *Journal of Internet Commerce*, 21(3), 150–166.
- [7] Zhang, Y. (2023). Artificial intelligence applications in cyber security. *International Journal of Information Technology*, 17(1), 89–104.