



National Conference- "Business 4.0: Redefining the Future of Business"

**A Study of Cyber Security Management in Online Shopping:
Marathwada region of Maharashtra**

Prof. Varunraj C. Kalse¹, Dr. Mohd. Farooque Khan²

¹Assistant Professor, Dept. of Management Science, Dr. Babasaheb Ambedkar Marathwada University, Sub-campus, Dharashiv

²Assistant Professor, Dept. of Management Science, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar.

ABSTRACT –

Consumers' views on internet buying are being influenced by cybersecurity concerns. In this technological age, online shopping has been integral to our daily lives. Cyber dangers and assaults are only going to increase in frequency and severity in tandem with the expansion of online purchasing. Hacking, theft of identities, along with credit card fraud is all on the rise due to the increasing number of people buying online. When it comes to cybersecurity, it's crucial to know what influences customer sentiment in order to establish trust and make buying a safe experience. Using a survey to examine several theories about significant cyber elements, this study investigates how customers' opinions toward online buying are impacted by cybersecurity. This study was conducted using a quantitative research technique. Like many other nations, the expanding nation of Marathwada region of Maharashtra in Southeast Asia has seen a rise in cyber threats and assaults in the last several years. Online shoppers in Marathwada region of Maharashtra are vulnerable to many of the same cyber dangers as shoppers anywhere else: phishing attacks, malware, data breaches, and more. Consumers' propensity to purchase online may be affected by their growing concerns about online security dangers caused by these cyber-attacks. In order to reduce cyber risk and increase customer confidence in online purchasing, it is crucial to determine what aspects of cyber security significantly affect consumers' views about online shopping. A deeper knowledge of the elements that impact Marathwada region of Maharashtra consumers' trust and involvement using online and e-commerce websites may be gained from the research study whose results are presented in this article using Multiple Regression Analysis. According to the findings, customer views regarding online buying are unaffected by demographic variables including age, gender, education level, and income. Consumers' perspectives on online purchasing are impacted by several aspects, including their employment position, level of cyber security awareness, the quality of the website, the security of the payment method, and concerns about data privacy.

Keywords: Cyber Security Management; Online Shopping; Marathwada Region Of Maharashtra; Multiple Regression Analysis; Cyber Risk

1. INTRODUCTION

Millions of people throughout the world rely on computers and mobile phones every day. These gadgets are being used for a variety of internet activities, such as shopping, banking, gaming, stock market, etc. People might fall prey to cyber-related fraud when they are unaware of the dangers posed by cybercrime [1]. People all across the globe are increasingly opting to purchase online rather than in physical stores. This shift is being spearheaded by e-commerce (online shopping) behemoths like Amazon, Alibaba, eBay, etc. One of the many ways technologies is improving people's lives is via making it easier to purchase online. Companies may enhance their supply chain activities, network, and customer and supplier services via e-commerce, which is widely recognized as a potent tool for business transformation [2]. Client data security is of utmost importance in today's rapidly evolving technology landscape across all industries, including banking, management, retail, communication, education, and shopping. Security is of the utmost importance in online banking due to the serious risk of unauthorized access to client data, which poses a threat to the bank's reputation and the ever-increasing prevalence of cybercrime perpetrated by the black hat community. Clients may collaborate with untrusted partners using more sophisticated and secure mechanisms [3].

Consumers' views on internet buying are being influenced by cybersecurity concerns. In this technological age, online shopping has been integral to our daily lives. Cyber dangers and assaults are only going to increase in frequency and severity in tandem with the expansion of online purchasing. Hacking, identity theft, along with credit card fraud are all on the rise due to the increasing number of people buying online. In order to establish confidence and establish a secure purchasing environment, it is crucial to comprehend the aspects of cybersecurity that impact customer sentiment [4]. The COVID-19 condition, which caused individuals to stay home more, was the primary driver of the rise in spending intensity. A new normal was denoted by this circumstance. The ease of online buying has made it a habit for certain people for quite some time. The online buying habits of Indonesians during the COVID-19 epidemic, with a focus on cybersecurity, will undoubtedly have community-wide ramifications [5]. With the rise of e-commerce in South Africa, driven by trends like more people shopping on mobile and more businesses advertising on social media, it's clear that a solid risk management

system is necessary [6]. Despite the obvious advantages, online buying can present some difficulties. This is because there are no brick-and-mortar establishments where customers and vendors may meet in person. When customers get an online purchase that doesn't meet their expectations, it's hard for them to complain over the phone or over email [7]. Online shopping apps' use on dispersed networks has been on the rise recently. One of the numerous benefits brought about by these apps is the ability to purchase online from anywhere. Offloading application data from user gadgets to servers presents several research problems, but it simplifies things overall [8].

When compared to other issues related to the internet, internet security ranks high among the most important in the modern day. Reason being, e-commerce and the transmission of information have both been radically altered by developments in technology, communications, and the cyber-Internet. So, it was critical to figure out how to secure online accounts, data, and information, as well as digital wallets and electronic money. All aspects of protecting data stored online, including online transactions, networks, and applications, are collectively referred to as "cybersecurity." [9]. E-commerce, or online shopping, has grown in importance in the modern economy as more and more companies move their operations online to tap into the worldwide consumer market. Some of the biggest and most lucrative businesses in the world today are those who conduct all of their operations online. The most critical component in ensuring the long-term viability of commercial organizations is managing risks in online transactions, as the expansion of e-commerce comes with a corresponding rise in risk exposure [10]. Online shopping refers to the marketing, sales, and distribution of goods and services conducted via the use of electronic means.

To put it simply, e-commerce refers to transactions that take place in an online setting. Electronic commerce encompasses any and all activities that take place in an online setting and have an effect on trade. Since it caters to clients all day, every day, in a wide variety of locations, e-commerce plays a crucial role in the exchange industry. When compared to traditional forms of trade, online shopping's novel structure is both more important and, in some cases, cheaper [11]. The spread of the Corona epidemic has accelerated the trend toward the widespread availability of internet services in this age of pervasive digitalization. The mobile service ecosystems is vulnerable to new threats brought about by the rapidly expanding mobile service industry. That being said, there are a lot of obstacles that mobile service providers must overcome in order to safeguard their services, especially the applications that go along with them. But app defenses are often only (weak) application-level security, including app monitoring while intrusion detection or app hardening [12]. The newest fad among millennials is online buying. The customer base has grown in tandem with the proliferation of new e-commerce applications. Just about everyone, especially the younger generation, is captivated by the idea of having local and international goods delivered to their home at a reasonably inexpensive price. Customers who are in a hurry to get the greatest discounts online don't seem to care about the growing number of cybercrimes, the danger of hackers, malware, ransomware attacks, etc. [13].

1.1 Research Objectives

Finding out what aspects of cyber security influence consumers' views on online buying is the primary goal of this study. By carrying out this research study, we want to accomplish the following primary goals:

- To learn about internet shoppers' worries about cybercrime in the Marathwada area of Maharashtra.
- To learn what makes people think about cyber security when they purchase online.
- To look at how these things affect internet buying habits in the Marathwada area of Maharashtra. The following are additional aims of this research study:
- To explore how consumers' past encounters with cyber security concerns influence their perspectives on online purchasing.
- To assess customers' level of knowledge about cyber security risks and how to mitigate them on the website.
- To provide policymakers and online companies in the Marathwada area of Maharashtra some pointers on how to fix cyber security issues and boost customer confidence when buying online.

1.2. Research questions

- Does the presence of security measures influence the probability that a consumer will make an investment from the online store?
- What is the correlation between privacy regulations and the probability of an online shopper making a purchase?
- Is the probability of completing an online purchase higher in countries with more stringent cyber laws and regulations? This study stands out because it takes a developing country's perspective on cybercrime and its effects on e-commerce technology.

1.3 Novelty of the paper

Using gender disparities and cybersecurity knowledge as focal points, this research offers a fresh look at how customers purchase online. This study delves into the specific difficulties encountered by buyers in a developing area, in contrast to earlier research that has mostly focused on industrialized economies. This research adds to our understanding of consumer behavior with cybersecurity in online commerce by analyzing these elements in a scenario that has not been thoroughly studied before. With their worries about cybercrime at the forefront of their minds, this study has the potential to

shed light on the online buying habits of Bangladeshi consumers. Additionally, governments and e-commerce companies in Bangladesh should use this study's results to address customers' worries about cyber security.

2. RELATED WORK

The purpose of that study is to investigate, in the context of the COVID-19 outbreak, how the people of Indonesia shopped online. A strategy that integrates cultural studies, economics, and digital law with cybersecurity research. Findings from that study highlight the social vulnerability consequences of Indonesians' penchant for heavy internet shopping. People may become isolated if they are immersed in a cultural setting. People, the four corners of their own being, the equipment and helpful objects used in the production of goods, and the consumable goods themselves are all alienated from one another by the nature of online shopping as productive labor. Although there was a potential for personal data to be exploited within the realm of security.

In order to adapt the framework to new dangers and technology developments, it is crucial to conduct constant research, as shown in the study [15]. Financial fraud, inefficient operations, cybersecurity threats, regulatory issues, and reputational concerns are just a few of the many concerns that the South African e-commerce business faces, according to key findings. To protect companies' and customers' interests, these results highlight the importance of a comprehensive risk management plan. In order to promote long-term development and increase customer trust, the report suggests measures to protect the e-commerce industry from these threats. There has to be continuous study into how risk management tactics affect customer behavior and market growth in the long run. The study concludes with a research- and analysis-based paradigm for South African e-commerce risk management.

Avoid falling victim to online shopping scams by reading [16] and putting that safety advice into practice before you buy anything. Working in tandem with the Justice Department, the Federal Trade Commission is a federal body in the United States responsible for enforcing antitrust civil laws and promoting consumer rights protection. The Federal Trade Commission said that in 2021, online shopping scams ranked second among all types of fraud. You may stay protected from these frauds by following these safety guidelines. Theft of personal information by cybercriminals allows them to commit fraud or make unlawful transactions. Theft of another person's personal identifying information, such as their social security number, bank account details, or credit card number, is known as identity theft. Theft of credit card information is a common tactic used by fraudsters, who will subsequently sell the returned monies or products. When combined with AI, machine learning is a fast-developing technology that has the potential to greatly improve the safety of online purchases and the level of awareness felt by shoppers.

There are two main goals to the research in [17]: first, to find out how different European nations do in terms of online shopping, and second, to identify the biggest obstacles to the growth of online shopping. In order to do that, they used a mixed-method approach that combined MCDA with a Likert-scale survey. One approach ranks the e-commerce success of European nations, while the other examines the challenges inherent to online purchasing. The study's findings reveal that various European nations place varying amounts of emphasis on cyber-security, and that within that continent; there are three distinct groups that pay varying amounts of focus on the most pressing problems with online trade. Denmark, Sweden, and the Netherlands are among the nations that respond well to online shopping. That proposal is a part of a larger plan for sustainable growth, which includes creating a trustworthy online space where companies and individuals may safely carry out their legal and personal freedoms. Finally, that research provides a theoretically new baseline for the literature on the current condition of e-commerce in Europe which takes into account the pandemic's consequences.

Five distinct algorithms—ECF, Behavioral Biometric Authentication, Adaptive Threat Intelligence, Transaction Anomaly Detection, with Dynamic Encryption Protocol—form a full-stack security architecture that was introduced in [18]. The DEP technique establishes a firm foundation for secure data transport by generating encryption keys dynamically during the user login process. For an additional degree of protection, behavioral biometric authentication employs DEP output to validate users according to their unique behavior. The ATI algorithm may continuously adapt security rules, offering a preventive barrier against new threats, by incorporating both current and prior threat information. TAD is very skilled in identifying suspicious activity in purchases made online, which contributes to the integrity of financial transactions. By combining their respective filtering capabilities, ECF and DEP make email transmission much more secure. Flowcharts are useful for understanding algorithms because they show how different algorithms interact with one another. Ablation research highlights the significance of each algorithm by revealing their individual contributions and how they interact to impact the entire safety posture. Based on performance tests utilizing several criteria, the proposed security framework surpasses the state-of-the-art with regard to effectiveness, flexibility, and usability.

Using trustworthiness as a moderating variable, the purpose of that research is to discover and assess customer consideration variables in online purchase choices [19]. Associative research describes that study. Participants were internet shoppers who were students at Universitas HKBP Nommensen Medan's Master of Management Postgraduate Program. They used a purposive selection strategy to choose 80 respondents for their sample. Questionnaires were used for primary data collection, while literature reviews were employed for secondary data gathering. In that research, the hypothesis was tested using an interaction test and linear regression analysis with a significance level of = 5% (0.05). Online purchase choices among Postgraduate Management program students were positively and significantly impacted by consumer consideration factors along with consumer confidence, according to the data. The impact of consumer consideration variables on online shopping choices was amplified by customer trust. When considering whether or not to purchase online, consumers give serious consideration to the following factors: pricing, product, transaction convenience, and transaction security. Customers have an easier time making purchases when businesses and individuals offering goods and services online are transparent and up-to-date with their pricing, product offerings, transaction security, and convenience policies.

The purpose of that study is to address some of the issues surrounding the choice to utilize the Shopee app [20]. This study examines the motivations behind students' usage of the Shopee app for making online purchases. Whether or not to utilize Shopee depends on how easy, secure, and trustworthy it

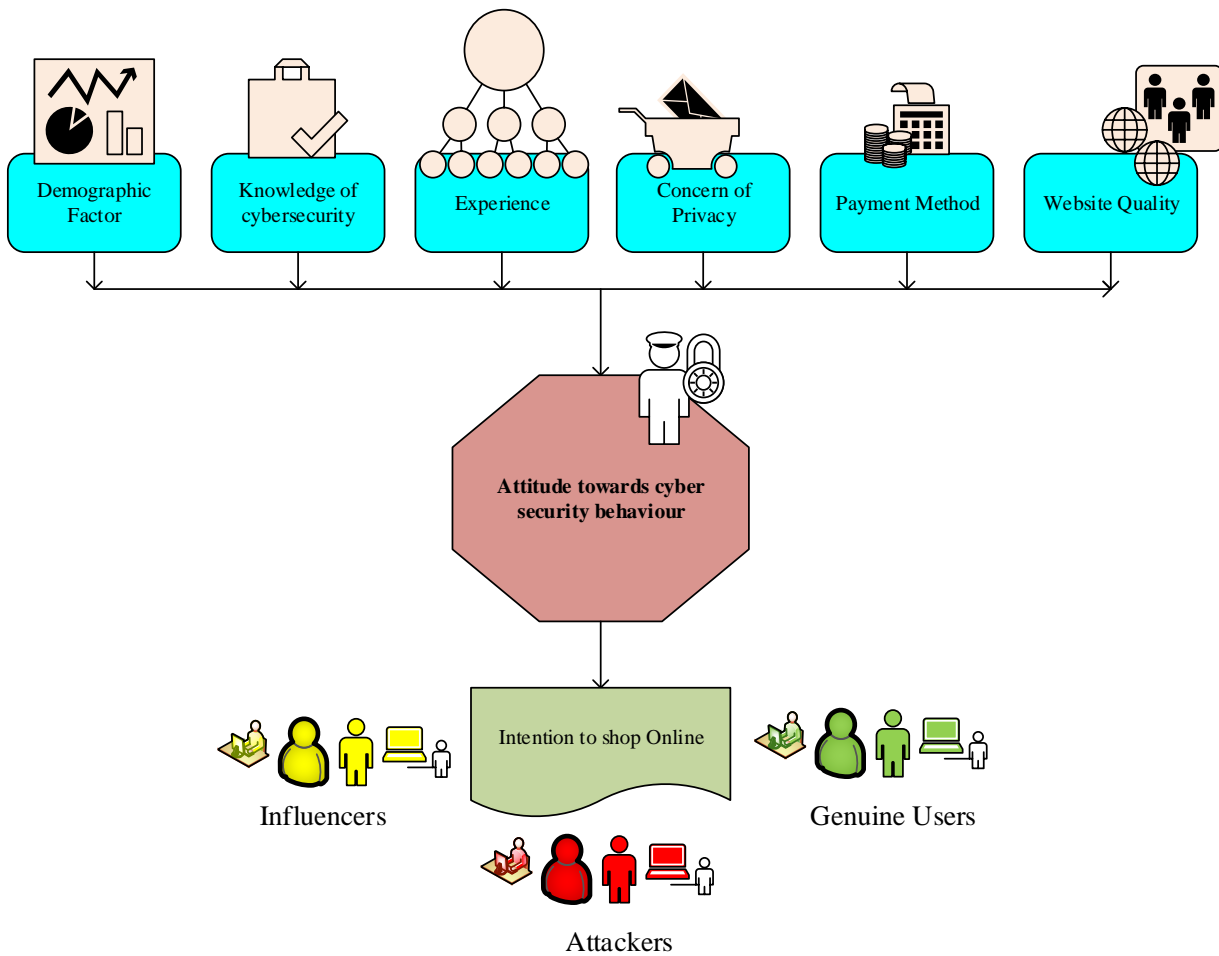
is. Students in their fifth and seventh semesters of management degrees at ITESA Muhammadiyah Semarang, Karya Husada University, along with Pandanaran University who utilize Shopee make up the population for that descriptive quantitative study. They used a random selection method to choose 100 respondents for their study. Processing data using SPSS version 25. That research found that the three factors mentioned above have an impact on whether or not people choose to utilize Shopee. Because of its high level of trust, ease of usage, and security during transactions, their study suggests that using Shopee is a great choice. Shopee is the most popular marketplace in Indonesia, therefore it's no surprise that many students utilize it.

3. Research gaps

While there is a wealth of information on how people purchase online, very little is known about how cybersecurity knowledge affects consumers' choices in poor nations like Marathwada region of Maharashtra. Furthermore, there have been conflicting findings on the relevance of gender differences in this setting. Some studies have shown significant inequalities, while others have not. These omissions highlight the need for further research on the relationship between gender, cybersecurity knowledge, and online purchasing habits in the Marathwada region of Maharashtra setting. Research has shown that online stores may benefit from high-quality websites and that customers are more likely to make purchases when the sites are easy to use. When looking specifically at Marathwada region of Maharashtra, however, studies investigating the connection among website quality and consumers' intents to purchase online are few.

4. Research approach and methods

Choosing the best approach to gather data for the study is what the research decision is all about. There are primarily two types of research methods: quantitative and qualitative. Decisions, especially in corporate contexts, benefit greatly from quantitative research methodologies. This study will use a quantitative research approach to collect useful data on the aspects pertaining to cybersecurity that impact customer attitudes towards online shopping in Marathwada region of Maharashtra.



Cybersecurity Management for Online Shopping

Fig.1.

4.1.1 Selection of research method

Following a quantitative research strategy comparable to those of prior studies will guarantee the consistency and dependability of the research findings. The quantitative research approach allows the researcher to gather data and examine it critically for the study. According to, quantitative research methods use mathematical, statistical, or computational tools to conduct organized and empirical investigations of specific phenomena. Consequently, in order to help make generalizable conclusions about a phenomena, quantitative research seeks to measure and evaluate the connection between variables.

4.1.2 Survey design

Using the Likert scale methods for scale design, a survey-type questionnaire was created for this investigation. Age, gender, income, work status, and educational attainment were used to construct the first section of the survey. The researcher was able to gauge customers' knowledge and views on cybersecurity in the digital space by analyzing the results of the survey's second section. We created Likert-type survey questions to help us identify and assess the variables of cybersecurity that impact customer opinions.

4.1.3 Likert scale coding

By emulating the format of Likert scale questions, which range from "strongly disagree" to "strongly agree," we may build our scale. There were five levels of coding for the measure, from 1 (strongly disagree) to 5 (strongly agree).

5. Data analysis

In this study, we will utilize statistical analysis tools like SPSS to examine the data collected from a survey, which will provide objective metrics. A systematic and empirical examination of a specific phenomenon using mathematical, statistical, or computer methods is at the heart of the quantitative research methodology. Hence, this research is going to employ SPSS software for statistical evaluation of the variables in order to examine their connection.

Variables	Numbers	Percentage
<u>Age</u>		
18-24	36	13.09
25-34	101	54.75
35-44	49	33.65
45-54	9	4.12
55-64	2	1.94
Missing	0	0.30
<u>Gender</u>		
Male	130	63.67
Female	68	31.17
Others	1	0.87
Missing	0	0.12
<u>Employment</u>		
Full time employee	100	54.25
Part time employee	27	13.22
Business	26	15.07
Not employment	43	21.66
Old age	3	1.77
Missing	0	0.15
<u>Income</u>		

25000	63	33.76
25000 – 50000	48	24.15
50000-75000	45	23.61
75000 – 100000	18	9.09
100000-125000	25	12.98
Null	0	0.12
Education		
I do not have any formal education	4	2.22
Completed high school (Year 12)	16	8.45
Bachelor	100	53.25
Masters	79	39.56
PhD	0	0.19

5.1 Multiple Regression Model

The purpose of this study is to examine the relationship between consumers' aversion to online shopping and their perceptions of cybercrime. The purpose of this research is to illuminate the relationship between customers' perceptions of cybercrime and various other trust characteristics that impact their inclination to engage in online commercial transactions. We have embraced TPB because it has been successfully used to examine e-commerce consumer behavior. In order to establish the connections between all of the independent variables, multiple regression was performed. Coefficients of correlation between variables are shown via the product-moment correlation (r) findings.

$$y_i = \beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \dots + \beta_p x_{ip} + \epsilon$$

where, for $i = n$ observations:

y_i = dependent variable

x_i = explanatory variables

β_0 = y-intercept (constant term)

β_p = slope coefficients for each explanatory variable

ϵ = an error term in the model (sometimes called the residuals)

An analyst may use data on several explanatory factors to make a prediction using the multiple regression model. Even yet, there are cases when the model is off by a small margin since actual results might vary from the model's predictions. To take these small deviations into consideration, the model incorporates a residual value, E , that reflects the discrepancy between the actual and studied outcomes.

The validity and reliability of the analysis are confirmed by using Cronbach's alpha and correlation. Two types of linear regression, basic and multiple, were used to analyze the data. The optimal determinants of consumers' intents to purchase online are their attitude toward behavior and their perceptions of the controls over their own behavior, as we demonstrate. Customers' actions are influenced by their level of confidence in both the seller and the internet medium. We go on to show that consumers' desire to buy is unaffected by subjective standards, online vendor confidence, cybercrime perception, or Internet trust, and that cybercrime has no effect on behavior either. Additionally, it has no moderating effect on the correlation between customers' confidence in e-commerce businesses and their propensity to make online purchases.

The dependability of a set of questions may be measured using Cronbach's Alpha, also known as tau-equivalent reliability. Each question that makes up the set is known as an item on the scale. In this way, Cronbach's alpha is a measure of a scale's dependability that takes into account its internal consistency. The reliability of a questionnaire, measured by Cronbach's Alpha, might range from 0 to 1. An indicator of a test's internal consistency is the average relationship among its items.

Intraclass correlations are shown by generalizability theory's G- and D-coefficients as well as Cronbach's alpha. As a means of estimating dependability, Hoyt converted the ratio of

$$r = \frac{MS_{\text{perisens}} - MS_{pi}}{MS_{\text{percoens}}}$$

where MS_{persons} is the person-by-item interaction mean square, and MS_{pi} is the person-by-variance mean square from an analysis of variance. Cronbach states that the formula that comes out of Hoyt's derivation is the same as alpha. Thus, split-half dependability is associated with intraclass correlations.

Table 2 Perceptions of online shopping

Secure payment gateway	Attitude toward online shopping					χ^2	df	p
	Very likely	Likely	Neither	Unlikely	Very unlikely			
Strongly agree	58[28.22]	22[45.80]	3[6.22]	0[0.52]	0[0.67]	147.72 16 <.001		
Agree	19[22.44]	79[54.43]	5[8.76]	0[0.98]	0[0.56]			
Neither agree nor disagree	[4.83]	6[7.34]	9[3.14]	1[0.23]	0[0.22]			
Disagree	0[1.49]	[2.33]	2[9.33]	0[0.56]	1[2.02]			

5.2 Hypothesis Testing

Hypothesis 1

The first hypothesis tests the idea that people's attitudes regarding internet buying are unaffected by their age. According to our study model, one personal aspect that affects consumers' attitudes towards internet purchasing is their age. In order to determine whether there is a relationship between age as well as mindset towards online purchasing, a Chi-square test of variability was conducted. The findings showed that there was no significant variation of age by deployed $\chi^2(20) = 27.85$, $p = 0.113$.

Hypothesis 2

Testing the significance of the correlation among website quality and one's attitude toward online purchasing is the focus of Hypothesis H2. To determine whether quality of the website and attitude toward online buying were unrelated, we used a Chi-square Test of Independence. Using 12 degrees of freedom, the Chi-square test yielded significant findings ($\chi^2(12) = 90.49$). The null hypothesis that the website quality has no correlation with attitude toward online purchasing is strongly refuted by the resultant p-value, which is less than 0.001.

Hypothesis 3

Consumers' opinions regarding online purchasing are unaffected by safe payment systems, according to Hypothesis H7. We used a Chi-square test of independence to see whether people's attitudes on online shopping and the use of secure payment systems were unrelated. According to the significant findings of the Chi-square test ($\chi^2(16) = 147.72$, $p < 0.001$), there is a relationship between attitudes towards purchasing goods online and safe payment methods. The findings are shown in Table 6, which demonstrates a relationship between views towards online shopping and safe payment solutions.

Here is a summary of the information gathered from 198 participants. Age, gender, occupation, income, and degree of education are among the variables gathered. For each demographic, we determined the frequency and percentage for age, gender, job position, income, and degree of education. According to the results, the largest demographic included in this study was those between the ages of 25 and 34 ($n = 101$, or 50.75 percent of those who filled out the survey).

6. Conclusion

In Marathwada region of Maharashtra, people's attitudes regarding online purchasing do not seem to be significantly affected by demographic criteria like age, gender, education level, and income, despite the fact that online shopping is becoming more popular. This study's results show that, in the setting of Marathwada region of Maharashtra, consumers' opinions regarding internet shopping are not significantly influenced by people's age. The results are consistent with those of other research that have similarly shown no correlation between age and perspective on internet buying. This research found no statistically significant correlation between having been the victim of a cyberattack in the past and being prepared to take precautions in the future. This result is noteworthy because it implies that customers could not always learn about dangers from their previous encounters, which is an important conclusion to draw from the research. Consumers are more inclined to continue purchasing since they have improved cybersecurity awareness and perceptions compared to pre-pandemic times, according to another important conclusion of this research.

REFERENCES

1. Alyousef, A. (2024). The impact of using artificial intelligence in online stores on consumers. *International Journal of Educational Sciences and Arts*.
2. (2021). Cyber Security Intelligence and Ethereum Blockchain Technology for E-commerce. *International Journal of Emerging Trends in Engineering Research*.
3. Manjula Bai, H. (2020). Perception Analysis of Online Shopping: A Case Study of amazon.com.
4. Zebari, D.A., & Asaad, R.R. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*.
5. Pramanik, R., & Prabhu, S. (2022). Analysing Cyber Security and Data Privacy Models for Decision Making among Indian Consumers in an e-commerce environment. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, 735-739.
6. Sai, G.A., Reddy, K.R., Gurunadh, K., Madhav, T.G., & M, B.B. (2024). eKart: A Cloud-Based E-commerce Platform for Shopping deployed on AWS. *2024 International Conference on Computational Intelligence and Computing Applications (ICCICA)*, 1, 531-535.
7. Khani, M., Fallah, Z., Bahlekeh, T., & Bai, N. (2020). The Consequences of the Identity Theft Fear in the Sport Products Online Shopping From the Perspective of Physical Education Students. *Annals of Applied Sport Science*.
8. Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A.S., Zhansetov, A., & Jumabaeva, S. (2020). Features of E-Commerce Risk Management in Modern Conditions. *Academy of Strategic Management Journal*, 19, 1.
9. Amoroso, E. (2023). BOT MANAGEMENT FOR ADVANCED CYBERSECURITY, ONLINE FRAUD PROTECTION, DATA AND SERVICE INTEGRITY FROM HUMAN.
10. Aljebrini, S. (2020). FACTORS INFLUENCING CONSUMERS ATTITUDE TOWARDS E-COMMERCE PURCHASE DECISION THROUGH ONLINE SHOPPING FOR UNIVERSITY STUDENTS IN PALESTINE.
11. Kont, K. (2024). The Role of Libraries in Creating a Safer Cyberspace: Awareness of Estonian Library Employees in Information Security. *International Information & Library Review*, 56, 135 - 149.
12. Fereidooni, H., Dmitrienko, A., Rieger, P., Miettinen, M., Sadeghi, A., & Madlener, F. (2022). FedCRI: Federated Mobile Cyber-Risk Intelligence. *Proceedings 2022 Network and Distributed System Security Symposium*.
13. Parveen, N., & Adak, R. (2019). Customer Awareness On Cyber Security Issues With Special Reference To Online Shopping: A Study Among Generation Y.
14. Setiyawan, R., & Prakasa, S.U. (2021). Indonesian Online Shopping Practices in the COVID-19 Pandemic Era: A Study of Culture and Cyber Security Law. *Jurnal Hukum Novelty*.
15. Malapane, T.A., & Ndlovu, N.K. (2024). Towards a Policy Framework for E-Commerce Risk Management: A Case of South African Online Shopping. *2024 Systems and Information Engineering Design Symposium (SIEDS)*, 96-101.
16. Malik, A.A. (2024). Online shopping, Cyber frauds and Fraud prevention Strategies. *International Journal for Electronic Crime Investigation*.
17. D'Adamo, I., González-Sánchez, R., Medina-Salgado, M.S., & Settembre-Blundo, D. (2021). E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability*.
18. Savya, S., Mohanraj, R., Sharada, K., Sachi, S., Neelima, K., & Ramadevi, P. (2024). Securing the Digital Commerce Spectrum and Cyber Security Strategies for Web, E-commerce, M-commerce, and E-mail Security. *Journal of Cybersecurity and Information Management*.
19. Nababan, T.S., Panjaitan, F., Panjaitan, R., Silaban, P., & H Silaban, P. (2021). Analysis of Consumer Consideration Factors on Moderated Purchase Decisions in Online Shopping By Consumer Trust (Study on Students of Master of Management Study Program, Postgraduate at HKBP Nommensen University, Medan). *Strategic: Journal of Management Sciences*.
20. Firmansyah, F., Setyawan, G.B., & Muslikhun, A. (2025). Analysis Of The Factors That Influence The Decision To Use The Shopee Application For Online Shopping Transactions. *Commercium : Journal of Business and Management*.