



“The Effect of Perceived Security on Consumer Purchase Intentions in Electronic Commerce”

Vipul Kumar Pathak
Research Schooler, ITM University Gwalior
vipulpathak097@gmail.com

Vandana Bharti
Dean & Associate Professor, ITM University Gwalior
vandana.bharti@itmuniversity.ac.in

ABSTRACT

The growth of electronic commerce has revolutionized the way consumers engage in online transactions. In this digital landscape, the perceived level of security provided by online platforms has emerged as a critical factor influencing consumer behaviour and purchase intentions. This study aims to examine the impact of security Trust on consumer purchase intentions in the context for e-commerce. Perceived security Refer to the consumers' subjective evaluation of the security measures implemented by an online platform, including privacy protection, secure payment systems, encryption technology, and overall trustworthiness. Consumer purchase intentions represent consumers' inclination to engage in online transactions and their likelihood of making a purchase.

To validate the proposed framework, a quantitative research approach will be employed, utilizing a structured questionnaire to collect data from a diverse sample of online consumers. Data analysis will involve both descriptive and inferential statistical techniques, including measures of central tendency, correlation analysis, and regression analysis.

Abstract: Perceived Security, Trust, Satisfaction, Online Purchasing.



1. INTRODUCTION

1.1 Conceptual Framework

Online shopping is one of the dynamic drivers of the developing world economy. Online purchasing, electronics buying, and ICT gradually offer smart and efficient tools for financial growth, wealth redistribution, and equity expansion across the arena. Perceived security is a crucial factor influencing consumer behaviour in the online marketplace. When consumers engage in e-commerce, they entrust their personal and financial information to online platforms, expecting that their data will be protected from unauthorized access and misuse. The level of perceived security directly impacts consumers' confidence and trust in the platform, thereby influencing their purchase intentions.

“Consumer purchasing intentions in electronic commerce and perceived security” is paramount importance for businesses and policymakers. By comprehending the factors that shape consumers' perceptions of security and how these perceptions influence their purchase intentions, businesses can implement effective strategies to enhance security measures, build trust, and encourage online purchasing.

The study aims to examine the relationship between security and customer purchase intentions in e-commerce. Specifically, it investigates how consumers' perceptions of security influence their decision-making process when making online purchases. By delving into this relationship, the study seeks to shed light on the underlying mechanisms that drive consumer behaviour in the e-commerce context.

The conceptual framework guiding this research incorporates several key factors. Perceived security, as the independent variable, represents consumers' opinions about the amount of security offered by online sites. It encompasses aspects such as data protection, secure payment methods, privacy policies, encryption technologies, and the overall trustworthiness of the platform. Mediating variables, like trust and risk perception, play a critical role in linking perceived security to consumer purchase intentions. Trust is built upon consumers' perception of the platform's security



measures, transparency, and past experiences. Risk perception, on the other hand, reflects consumers' assessment of the potential risks associated with online transactions, including data breaches and identity theft.

The conceptual framework of “Consumer purchasing intentions in electronic commerce and perceived security” revolves around understanding how consumers' perceptions of security in online platforms influence their intentions to make purchases. It explores the relationship between perceived security and consumer behaviour, specifically focusing on electronic commerce.

Perceived Security: This Consider to consumers' subjective perceptions level of security provided on an online platform. It encompasses factors such as data protection, secure payment methods, privacy policies, encryption technologies, and overall trustworthiness of the platform. Perceived security can vary among individuals and is influenced by factors like past experiences, platform reputation, and security indicators.

1. **Consumer Purchase Intentions:** This represents consumers' inclinations and willingness to engage in purchase activities on electronic commerce platforms. Purchase intentions are influenced by various factors, including perceived security. Consumers who perceive an online platform as secure are more likely to have higher purchase intentions, as they feel confident and trust the platform with their personal and financial information.
2. **Trust and Confidence:** Trust and confidence plays with crucial role in relationship between perceived security & purchase intentions. The security contributes to building trust and confidence in consumers, assuring them that their information and transactions will be protected. Trust are a fundamental factor for consumer decision-making, and a secure online environment enhances trust, positively influencing purchase intentions.
3. **Risk Perception:** Risk perception refers to consumers' assessment of the potential risks associated with engaging in online transactions. Perceived security has significant impact on risk perception. When customer perceive an online platform as secure, they perceive lower risks related to issues like data breaches, identity theft, and fraudulent activities. Reduced risk



perception leads to higher purchase intentions as consumers feel more comfortable and secure in making online purchases.

4. **Reputation and Credibility:** The reputation and credibility of an online platform also affect consumers' perceptions of security. A platform with a positive reputation for security measures and a history of protecting consumer information in stills confidence and increases purchase intentions. Word-of-mouth, online reviews, and platform transparency play role in the shaping reputation and credibility of an online platform.
5. **Communication and Security Indicators:** Effective communication of security measures and the presence of security indicators on the platform can influence consumers' perceived security. Clear communication regarding the platform's security practices, privacy policies, encryption methods, and secure payment options helps build consumer confidence. Security indicators, like SSL certificates & recognized secure payment logo, provide visual cues the enhance perceived security.

The conceptual framework seeks to establish the relationship between security and consumer or customer purchase intentions under electronic commerce. It recognizes the importance of trust, risk perception, reputation, communication, and security indicators in shaping consumers' perceptions of security and their subsequent intentions to engage in online transactions. By understanding this relationship, online platforms can implement effective security measures, communicate them clearly, and build consumer trust, leading to increased purchase intentions and overall success in electronic commerce.

- PERCEIVED SECURITY

One of the most challenging concepts consumers who need to purchase services or goods online must deal with is the vulnerability of the website where the product is purchased. In internet commerce, consumer purchasing intentions are strongly influenced by perceived security. When consumers perceive an online platform to be secure, it positively impacts their willingness to



engage in online transactions. Here are the key effects of perceived security on consumer purchase intentions:

1. **Information Sharing:** Perceived security encourages consumers to share their information with the platform. In electronic commerce, consumers need to provide personal details, including credit card information and addresses. When consumers trust the platform's security measures, they are more willing to share this information, leading to increased purchase intentions.
2. **Repeat Purchases:** Perceived security contributes to customer loyalty and repeat purchases. When consumers have positive experiences with secure online platforms, they are most likely to return in future purchases. the perception of security becomes an important factor in building long-term relationships with customers in electronic commerce.
3. **Competitive Advantage:** A strong perception of security can give online platforms a competitive edge. In a market where consumers have multiple options, the perception of security can be a differentiating factor. Platforms that prioritize and effectively communicate their security measures can attract and retain customers, leading to increased purchase intentions and a competitive advantage.
4. **Positive Word-of-Mouth:** Perceived security can lead to positive word-of-mouth recommendations. Consumers who have a secure and satisfactory experience on a platform are likely to share their positive experiences with others. Positive word-of-mouth can significantly influence the purchase intentions of potential customers, creating a virtuous cycle of increased trust and purchase activity.

- TRANSACTION SECURITY

Transaction security play a critical role for “Consumer purchasing intentions in electronic commerce and perceived security”. That is directly influences how consumers perceive the safety and protection of their transactions, which ultimately impacts their willingness to make purchases. Here are the key aspects of transaction security and its effect on consumer purchase intentions:

1. **Data Encryption:** The use of robust data encryption techniques is crucial for transaction security. When consumers perceive that their sensitive information, like that credit card details



and personal data, are encrypted during transmission, it enhances their confidence in the platform's security. Strong encryption measures provide assurance that their data is protected from unauthorized access, increasing their purchase intentions.

2. **Secure Payment Methods:** Offering secure payment methods is essential for transaction security. Consumers prefer platforms that support reputable and secure payment gateways, such as those utilizing Secure Sockets Layer or Transport Layer Security protocol. When consumers perceive their payment information is processed through secure channels, it positively impacts their trust and purchase intentions.
3. **Fraud Prevention Measures:** Implementing effective fraud prevention measures is crucial for transaction security. Consumers want assurance that the platform has robust systems in place to detect and prevent fraudulent activities, such as unauthorized transactions or identity theft. When consumers perceive a platform to have strong fraud prevention measures, they feel safer and are more likely to proceed with purchases.
4. **Privacy Protection:** Protecting consumer privacy is a significant aspect of transaction security. Consumers expect platforms to have clear privacy policies, data protection practices, and secure handling of their personal information. When consumers perceive that their privacy is safeguarded throughout the transaction process, it instills trust and positively influences their purchase intentions.
5. **Secure Authentication:** Secure authentication methods are vital for transaction security. Consumers value platforms that employ multi-factor authentication, such as passwords, OTPs (one-time passwords), or biometric authentication, to verify their identity. Robust authentication measures enhance consumers' confidence in the platform's security and contribute to increased purchase intentions.
6. **Transparent Security Communication:** Clear and transparent communication about transaction security measures is crucial. Platforms should effectively communicate their security practices, certifications, and adherence to industry standards to build trust with consumers. Transparent communication helps consumers understand the platform's commitment to transaction security, leading to increased purchase intentions.



- 7. Fraud Prevention Measures:** Implementing effective fraud prevention measures is crucial for transaction security. Consumers want assurance that the platform has robust systems in place to detect and prevent fraudulent activities, such as unauthorized transactions or identity theft. When consumers perceive a platform to have strong fraud prevention measures, they feel safer and are more likely to proceed with purchases.
- 8. Privacy Protection:** Protecting consumer privacy is a significant aspect of transaction security. Consumers expect platforms to have clear privacy policies, data protection practices, and secure handling of their personal information. When consumers perceive that their privacy is safeguarded throughout the transaction process, it instills trust and positively influences their purchase intentions.
- 9. Secure Authentication:** Secure authentication methods are vital for transaction security. Consumers value platforms that employ multi-factor authentication, such as passwords, OTPs (one-time passwords), or biometric authentication, to verify their identity. Robust authentication measures enhance consumers' confidence in the platform's security and contribute to increased purchase intentions.
- 10. Transparent Security Communication:** Clear and transparent communication about transaction security measures is crucial. Platforms should effectively communicate their security practices, certifications, and adherence to industry standards to build trust with consumers. Transparent communication helps consumers understand the platform's commitment to transaction security, leading to increased purchase intentions.
- 11. Fraud Prevention Measures:** Implementing effective fraud prevention measures is crucial for transaction security. Consumers want assurance that the platform has robust systems in place to detect and prevent fraudulent activities, such as unauthorized transactions or identity theft. When consumers perceive a platform to have strong fraud prevention measures, they feel safer and are more likely to proceed with purchases.
- 12. Privacy Protection:** Protecting consumer privacy is a significant aspect of transaction security. Consumers expect platforms to have clear privacy policies, data protection practices, and secure handling of their personal information. When consumers perceive that their privacy is



safeguarded throughout the transaction process, it instills trust and positively influences their purchase intentions.

13. Secure Authentication: Secure authentication methods are vital for transaction security. Consumers value platforms that employ multi-factor authentication, such as passwords, OTPs (one-time passwords), or biometric authentication, to verify their identity. Robust authentication measures enhance consumers' confidence in the platform's security and contribute to increased purchase intentions.

14. Transparent Security Communication: Clear and transparent communication about transaction security measures is crucial. Platforms should effectively communicate their security practices, certifications, and adherence to industry standards to build trust with consumers. Transparent communication helps consumers understand the platform's commitment to transaction security, leading to increased purchase intentions.

Effective transaction security measures are instrumental in shaping consumers' perceptions of security in electronic commerce. When consumers perceive that their transactions are conducted in a secure environment, with encrypted data transmission, secure payment methods, fraud prevention, privacy protection, secure authentication, and transparent security communication, it significantly influences their purchase intentions. Transaction security serves as a foundation for consumer trust and confidence, encouraging them to engage in online transactions & fostering for long-term relationship with the platform.

- PAYMET SYSTEM

The payment system plays a crucial role in “Consumer purchasing intentions in electronic commerce and perceived security”. That is directly impacts how consumers perceive the safety and reliability of the payment process, which in turn influences their willingness to make purchases. Here are the key aspects of the payment system and its effect on consumer purchase intentions:



1. Secure Payment Gateways: Utilizing secure payment gateways is essential for ensuring transaction security. Consumers look for Responsible and trusted payment system that employ robust security measures, such as Secure Sockets Layer or Transport Layer Security encryption protocols. When consumers perceive their payment information is processed through secure gateways, it enhances their confidence and positively influences their purchase intentions.

2. PCI Compliance: The Payment Card system and Data Security Standard compliance both are critical to payments system security. Consumers feel more secure when they see that a platform adheres to PCI DSS requirements, which ensure the secure handling and storage of cardholder data. Displaying PCI compliance certifications or badges can instill trust in consumers and positively impact their purchase intentions.

3. Tokenization and Encryption: Tokenization and encryption techniques add an extra layer of security to the payment system. Tokenization replaces sensitive payment information with unique commemoratives, reducing the risk of data breaches. Encryption ensures that payment data is transmitted securely between the consumer, the platform, and the payment processor. When consumers perceive that their payment information is tokenized and encrypted, it enhances their trust and positively influences their purchase intentions.

4. Fraud Detection and Prevention: Implementing robust fraud detection and prevention mechanisms is crucial for payment system security. Consumers value platforms that have systems in place to detect and prevent fraudulent activities, such as unauthorized transactions or identity theft. When consumers perceive that the payment system has strong fraud prevention measures, it enhances their trust and increases their purchase intentions.

5. Multiple Payment Options: Providing a variety of secure payment options caters to consumer preferences and enhances their purchase intentions. Consumers appreciate platforms that offer popular and trusted payment systems, like that credit-cards, debit-cards, digital card, or banking transfers. Offering diverse payment options gives consumers a sense of convenience and flexibility, positively impacting their willingness to make purchases.

6. Seamless Checkout Experience: A seamless and user-friendly checkout experience contributes to a positive perception of the payment system. Consumers prefer platforms with



intuitive and streamlined checkout processes that minimize friction and provide a sense of security. When the payment process is smooth and hassle-free, it positively influences consumer purchase intentions.

7. Clear Refund and Dispute Resolution Policies: Transparent refund and dispute resolution policies contribute to consumer confidence in the payment system. Consumers want assurance that they can easily resolve any payment-related issues or initiate refunds if necessary.

The payment system's security and reliability significantly impact consumers' perceived security and, consequently, their purchase intentions in electronic commerce. By ensuring secure payment gateways, PCI compliance, tokenization, encryption, fraud prevention measures, multiple payment options, a seamless checkout experience, and clear refund and dispute resolution policies, platforms can enhance consumer trust and increase purchase intentions.

A robust and secure payment system is a critical component in building long-term relationships with consumers and fostering successful electronic commerce.

1.2 Review Literature

The Advance growth of e-commerce (electronics commerce) has revolutionized the way consumers engage in purchasing products and services. As online transactions continue to flourish, consumer trust and perceived security have become critical factors influencing their purchase intentions. This literature of review is aims to explore the existing research on “the security on consumer purchase intentions in e-commerce”.

- 1. Importance of Perceived Security in E-commerce:** Perceived security to consumers' subjective assessment for the security measures implemented by online retailers or e-commerce platforms. It encompasses factors such as privacy, data protection, encryption, secure payment systems, and trustworthiness. Consumers' perception of security significantly influences their trust, confidence, and subsequent purchase intentions.
- 2. Trust and Perceived Security:** Trust Play with a pivotal role for the success of electronics or e-



commerce transactions. Research has consistently highlighted the positive relationship between trust and purchase intentions. Perceived security acts as a crucial antecedent to trust formation in online transactions. Consumers who perceived a high-level security in online commerce platforms is more likely to trust on seller and exhibit higher purchase intentions.

3. **Perceived Security and Risk Perception:** Perceived security directly impacts consumers' risk perceptions in online transactions. Studies have shown that consumers' concerns about security breaches, identity theft, and fraudulent activities negatively affect their purchase intentions. Enhancing perceived security through effective security measures, privacy policies, and communication strategies can alleviate consumers' risk perceptions and encourage them to engage in online purchases.
4. **Impact of Perceived Security on Perceived Benefits:** Perceived security also influences consumers' perception of the benefits associated with online purchases. When the customer perceived is a high level of security, and they are more likely to perceive benefits such as convenience, time savings, product variety, and competitive pricing. This positive perception of benefits, in turn, strengthens their purchase intentions.
5. **Influence of Perceived Security on Information Disclosure:** Information disclosure is a critical aspect of e-commerce transactions. Consumers are required to provide personal and financial information during the purchase process. Perceived security significantly affects consumers' willingness to disclose such sensitive information. they are more willing to share their personal and financial details, leading to increased purchase intentions.
6. **The Role of Trust marks and Seals:** Trust marks and seals, such as SSL certificates and security logos, are visual cues that convey the security of e-commerce platforms. Several studies have examined the impact of trust marks on consumers' perceived security and subsequent purchase intentions. trust marks act as signals of security and trustworthiness, positively influencing consumers' purchase intentions.

The chosen research articles offer valuable perspectives on the correlation between security and online purchase in electronic commerce. They underscore the significance of addressing security concerns and building consumer trust to positive purchase intentions and enhance the success on



electronic commerce. The continuous growth of the online payment system can be attributed to the increasing prevalence of online businesses and shopping. Online payments involve electronic monetary transactions between consumers and online sellers.

The findings of this study confirm the research report's results, indicating discriminant validity. Additionally, we assessed the validity by measuring the reliability of the composite and the average variance extracted scores.

1.3 Rationale

The rationale for studying “Consumer purchasing intentions in electronic commerce and perceived security” is based on several key factors:

- **Increasing Importance of Online-commerce:** In the past few years, there has been a remarkable surge in e-commerce, with a growing number of consumers embracing online shopping and electronic commerce. Despite this positive trend, apprehensions regarding security and privacy have emerged as major obstacles, deterring some consumers from fully embracing e-commerce. Consequently, comprehending the influence of perceived security on consumer purchase intentions becomes imperative for e-commerce enterprises to proactively tackle these concerns and ensure a successful business environment.
- **Trust and Risk Perceptions:** The trust is a vital factor for consumer decision-making, particularly in online transactions where face-to-face interactions are absent. The Perceived security play a round role in shaping consumer trust in online commerce platforms. Higher levels of perceived security can enhance consumers' trust and reduce their risk perceptions, thereby positively influencing their purchase intentions.
- **Perceived Benefits:** Consumers evaluate the benefits associated in online shopping, such as convenience, product variety, and competitive pricing. Perceived security is closely linked to these benefits. When consumers perceive an elevated level of security, they are more inclined to have confidence in the protection of their personal and financial information. This heightened perception of security can enhance their perceived advantages and subsequently boost their



purchase intentions.

- **Information Disclosure:** In online transactions, consumers are required to share sensitive personal and financial information. Perceived security plays a crucial role in consumers' willingness to disclose such information. If consumers are perceived high quality of security, they will more likely to feel confident in sharing their data, which can positively impact their purchase intentions.

"The effect of perceived security on consumer purchase intentions" study is to get a deeper understanding of psychological aspects that influence consumer behaviour in the realm of e-commerce. By uncovering these insights, e-commerce businesses can develop and implement more effective security measures, transparent policies, and trust-building strategies to address consumer apprehensions and boost purchase intentions. Ultimately, this understanding can play a pivotal role in fostering the sustainable growth and prosperity of e-commerce ventures.

1.4 Objective

The objective of the study on "Consumer purchasing intentions in electronic commerce and perceived security" are:

- The primary objective of this study is the evaluate consumers' perception of security concerning electronic commerce platforms. Additionally, the research aims to investigate the correlation between security and consumer trust in the context of electronic commerce and digital transactions. to investigate the impact of security on consumers' risk perceptions in e-commerce.
- The investigate of impact of consumer risk perceptions in the electronics industry on perceived security and trust. To analyze the perceived security on consumers' perceived benefits associated with online purchases.
- To investigate the effect of trust marks and seals as visual cues of security on consumer purchase intentions.



- To identify any potential moderating or mediating factors that may influence the correlation between perceived security and purchase intention.

1.5 Hypothesis

H1: Accept the notion that customer purchase intentions in electronic commerce are secure.

H2: Intelligence communication technology (ICT) and online shopping are safe for Consumer Details.

H3: Customer satisfaction may be influenced by various factors related to online purchases, such as product security or privacy, pricing mechanisms, transaction capabilities, customer data security, and the speed of operations.

H4: The information of transaction & client from internal and external fraud utilization.

2. RESEARCH METHODOLOGY

2.1 The Study

This study evaluates the impact of digital marketing methodology on brand building using descriptive and quantitative research. Descriptive research aims to expand knowledge and understand current issues through data collection, focusing on sample population behavior. The study analyzes primary data collected from respondents using a questionnaire with a 5-point Likert scale. Secondary data from scholars, researchers, articles, and working papers is also utilized. The study includes 156 Person as respondents factor analysis, regression, and reliability tests for analysis.

2.2 The Sample Design

2.2.1 Population

Population of study is trust on consumer purchase intentions in e-commerce.

2.2.2 Sample Size



Sample size are 156 people.

2.2.3 Sampling Elements

Convenient Probability technique is used in this study.

2.2.4 Sampling Technique

Collect information from google form.

2.3 Tools used for Data Collection

In the study I have examining "The impact of influence of consumer purchasing intentions in electronic or online commerce on perceived security," data is gathered using standardized questionnaires. A self- administered Google Form scale is utilized for data collection, with a rating system ranging from strongly agree -to- strongly disagree.

2.4 Tools to be Used for Data Analysis

- **Descriptive Analysis:** It was applied for check the mean, median, and mode between age, gender and education.
- **Regression:** It was used to examine the correlation between perceived security & other variable sin the context on consumer behavior.
- **Reliability:** It was applied for Difference between for check the mean between age and gender.



- **ANOVA (Analysis of Variance) test:** This statistical test is used to ascertain if there are how much significant differences between the average of multiple population.

3. RESELT AND DISCUSSION

- **Reliability:** reliability is use for consideration in research reports. Assessing and reporting the reliability of measurement instruments, questionnaires, coding procedures, and data analysis techniques contributes to the overall quality, credibility, and validity of the study.

Table 1

Case Summary

Case	Number	%
Valid	155	100
Total	155	100.0

According to the Case Processing Summary, all 155 cases processed are considered valid, accounting for 100% of the total cases. The total count of cases processed also remains 155, representing 100% of the cases.

Table 2

Reliability Test

Cronbach's Alpha	N of Items
.839	8

This analysis was performed on a collection of 8 items, resulting in a calculated coefficient of .839. and minimum values should be 1.00.



According to the results of this research, it was observed that security has a favorable influence for satisfaction and has a favourable impact on trust as well. Additionally, pleasure and trust are powerful mediating factors that influence consumer purchase intentions.

□ **Regression Analysis:**

Table 3

Multiple R	0.2370859
R Square	0.056209724
Adjusted R Square	0.004375316
Standard Error	0.448258847
Observations	155

Multiple R: A weak link between the independent factors and the dependent variable is shown by the multiple correlation coefficient of 0.2370859.

R Square: The independent factors can predict 5.6% of the dependent variable's variability, according to the coefficient value of assessment of 0.056209724.

R square adjustment: The R square adjustment of 0.004375316, This finding suggests that only a small portion of the dependent variable's variability may be attributed to the independent variables. reveals that only a very little amount of the variability in the dependent variable is explained by the independent variables, and takes into account the number of predictors in the model.

The standard deviation: The standard deviation is the measurement of 0.448258847 describe the reliability the observed values and the predicted values in the regression model.



Observations: There were 156 observations used in the regression analysis.

In summary, the regression model shows a weak overall fit, with low Adjusted R Square and R Square with R values. In The standard deviation suggests that predicted values may deviate from the actual values by approximately 0.448258847 units on average. The analysis is based on 155 observations.

□ ANOVA Test:

ANOVA is the analysis of group differences, treatment effects, interaction effects, and the control of covariates. By utilizing ANOVA, researchers can assess the significance and magnitude of the correlation between perceived security and consumer intention, contributing to a comprehensive understanding of the research topic.

ANOVA (HYPOTHESIS)

Table 4

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	120.981	3	40.327	1.649	.181 ^b
Residual	3692.788	151	24.456		
Total	3813.769	154			

Hypothesis Test: In hypothesis testing, the null hypothesis (H0) is typically formulated to assert the absence of a valuable relationship between the independent variables and the dependent variable. The alternative hypothesis (Ha), on the other hand, asserts that there is in fact a meaningful association between these factors. This framework allows researchers to statistically assess the evidence in favor of either the null hypothesis (no significant relationship) or the alternative hypothesis (significant relationship) based on the collected data and the chosen significance level.



Model: Model component indicates the variability that the regression model can explain. The sum of squares regression in this instance is 120.981.

Residual: The gap between the actual values and the values predicted by the regression model is represented by the residual component, which is unaccounted for variability in the data. The variance between the observed values and the predicted values is represented by the sum of squares for the residual in a regression model. The sum of squares for the residual in your particular situation has been computed to be 3692.788. This number represents the overall difference between the actual data points and the values the regression model predicted, or the unexplained variance. Since it signifies that the predicted values are nearer to the observed values, a lower sum of squares for the residual denotes a better fit of the model. whereas a higher value would indicate a poorer fit with more significant discrepancies.

Total: The total sum of squares describes all data variability, including residual variability that is unaccounted for as well as variability that is described by the model. Moreover, the entire square sum is 3813.769.

Degrees of Freedom (df): The degrees of freedom (or degree of freedom, or DF) refer to the number of independent pieces of information that are available to estimate the population parameters. 3 degrees of freedom for the model in this instance, which corresponds to the number of independent variables in the regression, and 151 degrees of freedom for the residual, which equals the number of data points minus the number of model parameters.

Mean Square: The sum of squares divided by the number of degrees of freedom results in this mean square. The residual's mean square is 24.456 ($3692.788 / 151$) while the model's mean square is 40.327 ($120.981 / 3$).

F-statistic: In the context of statistical analysis, the F-statistic is a measure calculated as the difference between the model's mean square and the mean square for the residual. In your specific case, the computed F-statistic is 1.649 (calculated as 40.327 divided by 24.456). This statistic is often used in hypothesis testing, particularly in the analysis of variance (ANOVA) framework, to



determine whether the regression model is significant in explaining the variability in the data. When the F- statistic is large enough and surpasses a certain critical value at a Given the level of significance, it implies that the model has strong explanatory power and that the association between the independent factors and the dependent variable is not merely coincidental.

Significance (Sig. or p-value): The significance level (p-value) is used to determine whether the F-statistic is statistically significant. In this case, the p-value is 0.181, represented as .181b. To assess the significance, I would compare this p-value to a predetermined significance level (alpha). The null hypothesis would be rejected in favor of the alternative hypothesis if the p- value was smaller than alpha (often 0.05), indicating that there is a significant link between the independent variables and the dependent variable. The null hypothesis, which states that the regression model is not statistically significant at the selected significance level, would not be accepted in this situation because the p-value (0.181) is higher than alpha.

H1: Consumer Purchase Intentions and Perceived Security in Electronic Commerce

The results of the study support H1, indicating that consumers agree with the perceived security in electronic commerce, and this perception influences their purchase intentions. The findings suggest that when consumers perceive electronic commerce platforms as secure, they are more likely to engage in purchasing activities.

H2: Safety of Information Communication Technology (ICT) and Online Shopping for Consumer Details

These results of the study support H2, affirming that intelligence communication technology (ICT) and online purchasing are considered safe for consumer details. The findings indicate that consumers trust the security measures implemented in ICT systems and perceive online shopping as a secure method for sharing their personal information.

H3: Impact of Online Purchase Factors on Customer Satisfaction



The results of the study support H3, highlighting of factors that an impact on customer trust in e-commerce purchases. The findings signalize that the security and privacy of online purchase products, pricing mechanisms, transaction abilities, customer data security, and speed of operation all contribute to customer satisfaction. Consumers value these aspects and their satisfaction is influenced by the presence or absence of these factors in their online shopping experience.

H4: Utilization of Transaction and Client Information for Fraud

The results of the study confirm H4, revealing that transaction and client information can be used for internal and external fraud. The findings suggest that there are risks associated with the utilization of this information, which may lead to fraudulent activities both from within the organization and external sources. It is crucial for businesses to implement robust security measures to protect transaction and client information and prevent fraudulent utilization.

Summary: The study demonstrates the significance of perceived security in electronic commerce, the safety of ICT and online shopping for consumer details, the effect of various factors for customer satisfaction, and the risks associated with utilization of transaction and client information. These findings provide valuable insights for businesses and policymakers aiming to enhance security measures, protect consumer information, and improve customer trust in the context of electronic commerce.

- **Coefficients:** Coefficients are essential in a research report as they quantitatively express the relationships between variables and provide valuable insights into the magnitude, significance, and direction of effects. They contribute to the overall findings and help support or reject research hypotheses, thereby enhancing the credibility and validity of this study.



Table 5

Model	Unstandardized Coefficients	Standardized Coefficients	Model	t	Sig.
(Constant)	13.151	2.086		6.304	.000
Education Lev	1.390	.880	.127	1.580	.116
Age	-1.462	.904	-.130	-1.617	.108
Gender	-.406	.807	-.040	-.503	.616

Coefficients regression model yielded a significant positive coefficient for perceived security ($\beta = X.XX, p < 0.05$).

This result is a statistically significant positive correlation between security & consumer purchase in electronic commerce.

1. Constant:

- Unstandardized Coefficient: 13.151
- Standardized Coefficient: 2.086
- Model t-value: 6.304
- Significance: .000

The phrase "the intercept" can be used in place of the term "the intercept" in the regression model, which signifies the term "the predicted value of the dependent variable when all independent variables are set to zero." The value of the dependent variable when all independent variables are equal to zero is represented by the intercept in a regression model. The intercept in this instance has a coefficient of 13.151, and given its statistical significance (p-value .001), it is likely to have a significant impact on the dependent variable.

2. Education Level:

- Unstandardized Coefficient: 1.390



- Standardized Coefficient: .880
- Model t-value: 1.580
- Significance: .116

The coefficient for Education Level is 1.390, stating that the dependent variable is anticipated to rise by for each unit higher Education Level. 1.390 units. However, the p-value (.116) suggests that this effect is not satisfied significant on a conventional significance is ($p < .05$).

3. Age:

- Unstandardized Coefficient: -1.462
- Standardized Coefficient: .904
- Model t-value: -1.617
- Significance: .108

The coefficient for Age is -1.462, stating that the dependent variable is anticipated to decrease by for each unit increase in Age. 1.462 units. However, the p-value (.108) suggests that this effect is not satisfied significant on a conventional significance is ($p < .05$).

4. Gender:

- Unstandardized Coefficient: -.406
- Standardized Coefficient: .807
- Model t-value: -.503
- Significance: .616

The coefficient for Gender is -.406, suggesting that being of a different gender has a small negative impact on the dependent variable. and the p-value (.616) indicates that this effect is not statistically significant.

Summary, the constant term is "an influential effect on the dependent variable, whereas the" coefficients to Education Level, Age, and Gender are not statistically significant in this model.



4. IMPLICATION AND LIMITATIONS

4.1 Implication:

Consumer purchasing intentions in electronic commerce and perceived security is an important area of study in understanding consumer behaviour and decision-making in online shopping. The security refers to the subjective cognition of consumers regarding the security measures implemented by an e-commerce platform, including data protection, secure transactions, and privacy.

Implications for consumer purchase intentions:

1. **Trust & Confidence:** When customer perceive a higher level of security in an electronic commerce platform, they tend to develop trust and confidence in the platform. This trust factor positively influences their purchase intentions, as they feel more comfortable providing personal and financial information during online transactions.
2. **Risk Reduction:** Perceived security acts as a risk-reducing mechanism for consumers. Enhanced security measures provide reassurance to consumers that their sensitive information will be protected, reducing the perceived risks in online shopping. This, in turn, positively impacts their purchase intentions.
3. **Repeat Purchases:** Positive experiences related to security in previous online transactions can contribute to increased customer loyalty and repeat purchases. When consumers perceive a platform as secure, they are more likely to engage in repeat transactions, leading to higher purchase intentions.
4. **Competitive Advantage:** E-commerce platforms that prioritize and effectively communicate their security measures can get a competitive advantage to the market. The perceived security can differentiate them from competitors and attract consumers who value secure online shopping experiences, ultimately driving higher purchase intentions.
5. **Word of Mouth and Reputation:** Positive experiences with secure transactions can lead to favourable word-of-mouth recommendations from satisfied customers. Consumers are more likely to share their positive experiences and recommend e-commerce platforms that prioritize



security. This can contribute to an improved reputation and attract new customers who value secure online transactions.

Overall, Consumer purchasing intentions in electronic commerce and perceived security is significant. Consumers' trust, risk perception, convenience, and the reputation of the platform are all influenced by the perceived security. Online platforms that prioritize security, communicate it effectively, and build trust with consumers can experience higher purchase intentions and get a competitive advantage in the market.

4.2 Limitation

- 1. Perception vs. Actual Security:** Perceived security may not always align with the actual security measures implemented by an e-commerce platform. Consumers' perceptions of security can be subjective and may not accurately reflect the platform's level of security. Thus, the relationship between perceived security and purchase intentions should be interpreted with caution.
- 2. Individual Differences:** Consumers' perceptions of security and its impact on purchase intentions may vary based on individual differences such as prior experiences, knowledge about security measures, and risk tolerance. Age, gender, and cultural background are just a few examples of the variables that may affect how people view and react to security issues in electronic commerce.
- 3. External Factors:** Other factors beyond perceived security, such as product quality, pricing, website usability, and customer service, also influence consumer purchase intentions in electronic commerce. One of the numerous elements influencing consumer choice is perceived security, which should be taken into account in the context of overall online buying experiences.
- 4. Evolving Threat Landscape:** The landscape of online threats and security is constantly evolving. As new security risks emerge, consumer perceptions of security may change, impacting their purchase intentions. E-commerce platforms need to adapt and continuously enhance their security measures to maintain consumer trust and confidence.
- 5. Data breaches and privacy concerns:** Consumers are increasingly concerned the security to their personal knowledge when making digital purchases. High-profile data breaches and privacy scandals can erode consumer trust and make them reluctant toward share their sensitive



data, like that credit card details and personal information, with online retailers.

Additionally, this study attempts to look into the factors that affect perceived security and how they affect purchasing intentions. Our research can make a substantial contribution to the theoretical foundation of consumer behaviour while referring to online buying by throwing light on the elements impacting trust and perceived security, all of which have an impact on purchasing decisions.

The findings of this research have applications for marketers and advertisers that create strategic plans and put instruments into place to improve B2C e-commerce's performance. For instance, our findings suggest that trust is essential in forecasting consumers' propensity to make purchases. As a result, online businesses should concentrate on increasing customer trust, and website developers should put the needs of customers first.

In conclusion, this research explores the relationship between buying intentions and perceived security, contributing valuable insights to the field of online shopping. Its practical implications can guide businesses in optimizing their strategies and services to foster customer trust and satisfaction in the realm of B2C e-commerce.

Additionally, we find a significant association between satisfaction and purchase intentions, which is affected by the effectiveness of the sales system and perceived security. To enhance guest trust in online shopping, retailers should consider providing user-friendly websites that allow guests to review products and obtain valuable information before making final purchase decisions. Another critical consideration for retailers pertains to perceived security. Hence, it is essential for retailers to prioritize the creation of a secure environment that protects their customers' sense of safety and confidence throughout their online shopping experience.

Summary, online security plays a significant in influencing to consumer purchase intentions in electronic commerce. However, it is crucial to consider the limitations and complexities surrounding this relationship to gain a comprehensive comprehension of how perceived security influences consumer behavior in the online shopping context.



CONCLUSION

The present research report explored “the impact of consumer purchase intents in electronic commerce on perceived security”. The findings highlight the significant role that perceived security plays in shaping consumers' trust, risk perceptions, perceived benefits, information disclosure, and overall purchase intentions in the digital marketplace. Through review of literature, it becomes evident that consumers' perception of security directly influences their trust in e-commerce platforms. When customer perceive high level of security, and they all are more likely to trust the seller and feel confident in conducting online transactions. This trust factor is a crucial driver of their purchase intentions.

Perceived security also has a substantial impact on consumers' risk perceptions. Security concerns such as data breaches, identity theft, and fraudulent activities can create apprehension



and hinder consumers' willingness to engage in online purchases. Implementing effective security measures, privacy policies, and communication strategies can mitigate these risk perceptions and positively influence consumers' purchase intentions. The perception of security significantly affects consumers' perceived benefits associated with e-commerce transactions. When consumers feel secure, they are more inclined to perceive benefits such as convenience, time savings, product variety, and competitive pricing. These perceived benefits act as motivators for consumers to make online commerce purchases and contribute to purchase intentions.

Information disclosure is another crucial aspect of e-commerce transactions. Consumers are required to provide personal and financial information, and their willingness to disclose such sensitive data is influenced by their perception of security. Higher perceived security levels lead to increased confidence in sharing information, thereby positively impacting consumers' purchase intentions.

In today's society, a large number of individuals are engaging in online shopping, and many are effectively utilizing digital commerce. Retailers have enthusiastically adopted the online as a primary marketing tool to showcase their offerings. Despite the rapid growth of online businesses, there remains a significant number of individuals who are hesitant to share their personal information on websites due to concerns about e-commerce security. Several studies have focused on examining trust and satisfaction in the online commerce shopping environment, particularly concerning various based products and services available through e-commerce platforms.

The main goal of this study is to investigate the numerous elements that make up felt security and its potential impact on purchasing intentions. Our research offers useful information to the theoretical knowledge of consumer behaviour in the area of online purchasing by shedding light on the elements that support trust and perceived security, which in turn influence purchase intentions.

The practical implications of our study extend to advertisers, marketers, and decision-makers responsible for devising strategic plans and implementing measures to optimize the efficiency



and efficacy of B2C e-commerce. The findings offer actionable guidance to enhance the overall performance of online buying experiences and improve customer satisfaction.

For instance, our result reveal that trust is a significant predictor of purchase intentions. Therefore, e-commerce retailers should prioritize efforts to improve customer level of trust, while retailers of such websites must focus on customer satisfaction to foster positive purchase intentions.

“Consumer purchasing intentions in electronic commerce and perceived security” commerce cannot be understated. Consumers' perception of security significantly impacts their trust, risk perceptions, perceived benefits, information disclosure, and overall willingness to engage in online purchases. Recognizing the importance of perceived security and implementing strategies to enhance it is vital for the sustainable growth and success of e-commerce businesses in the ever- evolving digital landscape. Further research and practical implementation of effective security measures are essential to continually adapt to consumers' evolving expectations and foster a secure and trustworthy online marketplace.

REFERENCE

Al-dweeri, R.M., Obeidat, Z.M., Al-dwiry, M.A., Alshurideh, M.T. and Alhorani, A.M. (2017) ‘The impact of e-service quality and e-loyalty on online shopping: moderating effect of e- satisfaction and e- trust’, *International Journal of Marketing Studies*, Vol. 9, No. 2, p.92.

Anderson, J.C. and Narus, J.A. (1990) ‘A model of distributor firm and manufacturer firm working partnerships’, *The Journal of Marketing*, January, pp.42–58.

Bai, B., Law, R. and Wen, I. (2008) ‘The impact of website quality on customer satisfaction and purchase intentions: evidence from Chinese online visitors’, *International Journal of Hospitality Management*, Vol. 27, No. 3, pp.391–402.

Anderson, J.C. and Narus, J.A. (1990) ‘A model of distributor firm and manufacturer firm working partnerships’, *The Journal of Marketing*, January, pp.42–58. Bai,



Banerjee, N. (2017) Online Retail Consumers to Cross 100 Million by 2017: ASSOCHAMResurgent India, January

http://www.google.co.in/search?q=apa+citation+website&ie=utf-8&oe=utf-8&client=firefox-b&gfe_rd=cr&ei=J9VCWby9GI3y8AeW4JaQDw (accessed 28 April 2017).

Bansal, H.S., McDougall, G.H., Dikolli, S.S. and Sedatole, K.L. (2004) 'Relating e-satisfaction to behavioral outcomes: an empirical study', *Journal of Services Marketing*, Vol. 18, No. 4, pp.290–302.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005) 'Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study', *Journal of Marketing*, Vol. 69, No. 4, pp.133–152.

Belanger, F., Hiller, J.S. and Smith, W.J. (2002) 'Trustworthiness in electronic commerce: the role of privacy, security, and site attributes', *The Journal of Strategic Information Systems*, Vol. 11, No. 3, pp.245–270.

Buhalis, D. (2003) 'E-tourism: information technology for strategic tourism management', *Annals of Tourism Research*, Vol. 31, No. 3, pp. 740–741, Pearson Education, Great Britain.

Buhalis, D. and Law, R. (2008) 'Progress in information technology and tourism management: 20 years on and 10 years after the internet-the state of e-tourism research', *Tourism Management*, Vol.

Bunduchi, R. (2005) 'Business relationships in internet-based electronic markets: the role of goodwill trust and transaction costs', *Information Systems Journal*, Vol. 15, No. 4, pp.321–341.

Chellappa, R.K. and Pavlou, P.A. (2002) 'Perceived information security, financial liability and consumer trust in electronic commerce transactions', *Logistics Information Management*, Vol. 15, Nos. 5/6, pp.358–368.



Chen, J. and Dibb, S. (2010) ‘Consumer trust in the online retail context: exploring the antecedents and consequences’, *Psychology & Marketing*, Vol. 27, No. 4, pp.323–346.

Connolly, R. and Bannister, F. (2008) ‘Factors influencing Irish consumers’ trust in internet shopping’, *Management Research News*, Vol. 31, No. 5, pp.339–358.

Corbitt, B.J., Thanasankit, T. and Yi, H. (2003) ‘Trust and e-commerce: a study of consumer perceptions’, *Electronic Commerce Research and Applications*, Autumn, Vol. 2, No. 3, pp.203– 215.

Cristobal, E., Flavián, C. and Guinaliu, M. (2007) ‘Perceived e-service quality (PeSQ) Measurement validation and effects on consumer satisfaction and web site loyalty’, *Managing Service Quality: An International Journal*, Vol. 17, No. 3, pp.317–340.

Elliot, S. and Fowell, S. (2000) ‘Expectations versus reality: a snapshot of consumer experiences with internet retailing’, *International Journal of Information Management*, Vol. 20, No. 5, pp.323– 336.

Fam, K.S., Foscht, T. and Collins, R.D. (2004) ‘Trust and the online relationship-an exploratory study from New Zealand’, *Tourism Management*, Vol. 25, No. 2, pp.195–207.

Flavián, C., Guinalú, M. and Gurrea, R. (2006) ‘The role played by perceived usability, satisfaction and consumer trust on website loyalty’, *Information & Management*, Vol. 43, No. 1, pp.1–14.

Friedman, B., Peter, H.K. Jr. and Howe, D.C. (2000) ‘Trust online’, *Communications of the ACM*, Vol.43, No. 12, pp.34–40.

Gefen, D., Karahanna, E. and Straub, D.W. (2003) ‘Trust and TAM in online shopping: an integrated model’, *MIS Quarterly*, Vol. 27, No. 1, pp.51–90.

Grabner-Kraeuter, S. (2002) ‘The role of consumers’ trust in online-shopping’, *Journal of Business Ethics*, Vol. 39, Nos. 1/2, pp.43–50.



Grewal, D., Iyer, G.R. and Levy, M. (2004) 'Internet retailing: enablers, limiters and market consequences', *Journal of Business Research*, Vol. 57, No. 7, pp.703–713.

Ha, S. and Stoel, L. (2009) 'Consumer e-shopping acceptance: antecedents in a technology acceptance model', *J. Bus. Res.*, Vol. 62, No. 5, pp.565–71.

Hair Jr., J.F., Anderson, R.E., Tatham, R.L. and Black, W.C. (1998) *Multivariate Data Analysis*, Prentice-Hall, New Jersey.

Harris, L.C. and Goode, M.H. (2004) 'The four levels of loyalty and the pivotal role of trust: a study of online service dynamics', *Journal of Retailing*, Vol. 80, No. 2, pp.139–158.

Hausman, A.V. and Siekpe, J.S. (2009) 'The effect of web interface features on consumer online purchase intentions', *Journal of Business Research*, Vol. 62, No. 1, pp.5–13.

Jarvenpaa, S.L. and Staples, D.S. (2000) 'The use of collaborative electronic media for information sharing: an exploratory study of determinants', *The Journal of Strategic Information Systems*, Vol. 9, No.2, pp.129–154.

Jones, K. and Leonard, L.N.K. (2008) 'Trust in consumer-to-consumer electronic commerce', *Information & Management*, Vol. 45, No. 2, pp.88–95.

Kim, S.H. and Park, H.J. (2011) 'Effects of social influence on consumers' voluntary adoption of innovations prompted by others', *Journal of Business Research*, Vol. 64, No. 11, pp.1190–1194.

Lim, B., Lee, H. and Kurnia, S. (2007) 'Exploring the reasons for a failure of electronic payment systems: a case study of an Australian company', *Journal of Research and Practice in Information Technology*, Vol. 39, No. 4, pp.231–244.