# EFFECT OF RISK PERCEPTION ON CONSUMER ONLINE PURCHASE INTENTIONS IN THE E-COMMERCE INDUSTRY IN ABUJA FCT

**[1]AJIBADE, Patricia Ajoke, [2]AHMED Abdullahi Ibrahim PhD, [3]ABDUL Adamu PhD**
[1,2&3]Department of Business Administration, Nasarawa State University, Keffi
Email:ajibade.patricia2015@gmail.com & ibrahimahmedabdullahi@nsuk.edu.ng

**Abstract**
*This study assessed the effect risk perception on consumer online purchase intentions in the e-commerce industry in Abuja FCT. The study's specific objectives were to assess the influence of product risk, and security risk on consumer online purchase intentions in the e-commerce industry in Abuja FCT. A sample size of 425 individuals residing in the Federal Capital Territory (FCT) Abuja who have access to the internet and have either made online purchases or have shown interest in online shopping within the past year were selected using the Cochran (1963) formula for sample size determination. Purposive and convenience sampling methods were employed in selecting the respondents. Data was collected through primary sources using a structured questionnaire on a five-point Likert scale. Structural equation modeling with partial least squares (PLS-SEM) was employed to analyse the data and test hypotheses. The results show that product risk has a positive but insignificant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT, while security risk revealed a negative significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT. The study concludes that risk perception has a significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT. The study recommends that E-commerce businesses should invest in advanced cybersecurity measures such as SSL encryption, multi-factor authentication, and fraud detection systems. Businesses should still enhance product transparency and consumer trust by providing detailed product descriptions, high-resolution images, and authentic customer reviews.*
**Keywords:** *Risk Perception, Product Risk, Security Risk, E-Commerce Industry, Abuja*

## Introduction

The exponential growth of e-commerce has fundamentally transformed the global retail landscape, with worldwide e-commerce sales reaching $5.2 trillion in 2021 and projected to exceed $8.1 trillion by 2026 (Smith & Jones, 2023). This digital transformation in retail has been particularly accelerated by the COVID-19 pandemic, which forced both businesses and consumers to embrace online shopping platforms at an unprecedented rate. Despite these promising growth trends, consumer risk perception remains a critical factor influencing online purchase intentions across global markets. In developed economies, studies have shown that approximately 70% of potential online purchases are abandoned due to various perceived risks (Anderson et al., 2022). Product risk, which encompasses concerns about product quality, authenticity, and alignment with online descriptions, continues to be a primary barrier to e-commerce adoption. For instance, in the European Union, nearly 45% of consumers report hesitation in online purchasing due to concerns about product authenticity and quality assurance (European Consumer Report, 2023). Security risk, another crucial dimension, has become increasingly prominent in the digital marketplace. Global cybersecurity reports indicate that e-commerce platforms experienced a 40% increase in security breaches between 2020 and 2023, affecting consumer confidence in online transactions (Watson & Lee, 2023). The rise in sophisticated cyber threats has heightened consumer awareness about the security of their personal and financial information during online transactions.

In the African context, e-commerce has shown remarkable growth, with the continent's e-commerce market value reaching $37 billion in 2023 (African Development Bank, 2023). Countries like Nigeria, South Africa, and Kenya have emerged as leading e-commerce markets in the region. However, the adoption rate faces unique challenges related to risk perception. Studies across African markets indicate that 65% of potential online shoppers express significant concerns about both product authenticity and transaction security (Mohammed & Okonkwo, 2022). Nigeria, as Africa's largest economy and most populous nation, has witnessed substantial growth in its e-commerce sector. The country's e-commerce

market was valued at $13 billion in 2023, with a projected annual growth rate of 15% (Nigerian Bureau of Statistics, 2023). However, the sector faces distinctive challenges, particularly in urban centers like Abuja FCT, where despite higher internet penetration and digital literacy rates, consumer risk perception remains a significant barrier to e-commerce adoption.

In Abuja FCT, the capital city's growing middle class and technological infrastructure present significant opportunities for e-commerce growth. However, recent studies indicate that approximately 58% of Abuja residents express concerns about product reliability in online shopping, while 62% worry about transaction security (Ibrahim & Nnamdi, 2023). These statistics underscore the critical need to understand how risk perception influences online purchase intentions in this important market.

E-commerce platforms have made significant strides in building consumer trust through various initiatives, yet perceived risks continue to affect online purchase behavior. These platforms have implemented comprehensive measures including secure payment systems, product warranties, consumer-friendly return policies, and enhanced data protection protocols to boost consumer confidence (Gefen & Straub, 2024). In Nigeria, major e-commerce players like Jumia and Konga have introduced features such as customer reviews, cash-on-delivery options, and improved delivery systems to address concerns about product quality, payment security, and delivery reliability.

Nevertheless, consumer apprehension persists, particularly in Abuja FCT, where these measures have not fully alleviated perceived risks. Concerns about product authenticity, transaction security, and delivery reliability continue to influence purchase decisions. The presence of security risks related to personal and financial data, coupled with product risks concerning authenticity and quality, undermines consumer confidence in digital commerce. These persistent concerns have led to hesitancy in online shopping, thereby limiting the growth potential of the e-commerce sector.

Contemporary research has extensively examined risk perception's influence on online purchase intentions, particularly in emerging markets where trust issues significantly impact e-commerce growth. Park et al. (2021) demonstrated that in Southeast Asian markets, concerns about financial fraud and data breaches substantially reduce consumers' willingness to engage in online transactions. In South Africa, Hassan and Ali (2022) revealed that uncertainties surrounding product authenticity and data privacy significantly deter online shopping adoption. Additionally, Singh et al. (2023) identified how social and psychological risk factors in India create barriers to consumer engagement in e-commerce through increased anxiety and mistrust.

While existing research provides valuable insights into specific risk categories affecting online purchases, most studies have focused on isolated risk factors rather than adopting a holistic approach. Chen and Widjaja (2022) demonstrated that addressing financial and security concerns alone was insufficient in reducing overall perceived risk, as social and product-related factors played equally important roles. Li and Zhang (2023), while examining psychological risks in the U.S. e-commerce market, highlighted the need for similar studies in emerging markets, particularly in Sub-Saharan Africa.

This research aims to address the gap in existing literature by examining the combined effects of product and security risks on consumer online purchase intentions, specifically within Abuja FCT's e-commerce sector. By focusing on these key risk dimensions, the study seeks to provide a more comprehensive understanding of how risk perception influences online shopping behavior in this emerging market.

The main objective of this study is to access the effect of risk perception on consumer online purchase intentions in the e-commerce industry in Abuja FCT while the specific objectives are to:

i. determine the effect of product risk on consumer online purchase intentions in the e-commerce industry in Abuja FCT; and
ii. identify the effect of security risk on consumer online purchase intentions in the e-commerce industry in Abuja FCT

The following hypotheses guided the study:
**$H_{01}$:** product risk has no significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT
**$H_{02}$:** security risk has no significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT

## LITERATURE REVIEW

### Risk Perception

Risk perception has been conceptualized differently by various scholars in the context of e-commerce and consumer behavior. Mitchell and Harris (2022) define risk perception as the subjective judgment that consumers make about the potential negative consequences and uncertainty associated with their purchase decisions in online environments. Taking a psychological perspective, Zhang and Thompson (2023) characterize risk perception as a cognitive process through which individuals evaluate and assess potential threats or losses associated with a particular action or decision, influenced by both personal experiences and social factors. In a more comprehensive definition focusing on e-commerce, Abdullah and Kumar (2021) describe risk perception as the degree to which a consumer believes that using online shopping platforms could lead to negative outcomes, including financial losses, product disappointment, privacy breaches, or psychological discomfort, which shapes their attitudes and behavioral intentions toward online transactions.

### Product Risk

Zhang and Wang (2019) defined product risk through the lens of digital transformation, characterizing it as the uncertainty associated with integrating digital technologies into traditional product offerings and the potential for cybersecurity vulnerabilities that could compromise product functionality. The emergence of artificial intelligence has prompted scholars like Lee and Kim (2022) to conceptualize product risk as the potential for algorithmic bias and decision-making errors in AI-enabled products, emphasizing the ethical implications and reliability concerns of autonomous systems. This perspective has been complemented by Cohen et al. (2021) who frame product risk in terms of data privacy and consumer trust, particularly focusing on smart products and connected devices.

### Security Risk

Security risk often encompasses the potential for unauthorized access to consumer data during online transactions. Studies highlight how consumer concerns about data breaches, where personal or financial information could be stolen, significantly deter online purchasing intentions (Wang et al., 2022). This risk arises from hacking, phishing, or weak data protection mechanisms implemented by online retailers (Chen & Zhou, 2023). Security risk also relates to concerns about the safety of financial transactions. For example, consumers worry that their payment details may be intercepted by cybercriminals, leading to fraud or identity theft, a factor that has been shown to influence their hesitation to shop online (Lin & Fang, 2023).

### Online Purchase Intention

Online Purchase Intention refers to the consumer's willingness and likelihood to engage in purchasing transactions through internet platforms. According to Wang and Chang (2023), it represents the strength of a consumer's intention to perform a specified online buying behavior and indicates the probability that the consumer will follow through with an online purchase. Park et al. (2022) expands this definition by describing it as a situation where a consumer is willing and intends to make online transactions, demonstrating the consumer's desire to be involved in online shopping activities.

### Empirical Review

Abdullahi et al. (2023) examines the effect of the perceived risk dimension on online buying behaviour. The population of this study constitutes undergraduate students of ABUBS. The number of departments in ABUBS is (six) 6 they are Accounting, Business Administration, Banking and Finance, Economics, Insurance and Actuarial Science and Marketing. The sample size of 246 was determined using Yamane

(1973) formula. In this study, simple random sampling was employed. Date was collected through self-administered questionnaire. This study employs the use of Statistical Package for the Social Sciences (SPSS) version 21 for data coding, data screening, and other preliminary analyses. However, for the major analysis, the study employs the use of Partial Least Squares Structural Equation Modeling (PLS- SEM) path modeling using the smartPLS3.2.7 statistical software. The findings of the study showed that financial risk and privacy risk in online buying behavior were found to be negative and significant. However, Product risk was found to be a positive and insignificant relationship in online buying behavior. The study was conducted on students at public university while the current study encompasses a broader scope.

Mayo and Layante (2022) examined the level of online shoppers' intention towards online purchases as affected by perceived risks. The study used descriptive-correlational design to describe the extent of perceived risks in terms of product, financial, security, social, and time risk and the level of purchase intention of the participants. A total of 198 selected public-school teachers in Calapan City were selected to ask participation in the survey to assess their five types of risk perceptions and online purchase intentions. Data were collected with the aid of online survey instruments. Results indicated a significant relationship between the extent of the perceived risks by the selected public-school teachers in Calapan City in terms of product, financial, security, social, and time risk and the level of their purchase intention. Moreover, the result of the study shows that despite the risks they perceive in online shopping, they are still interested in online shopping, use it frequently, and consider shopping online more than shopping at physical stores. Although this study is comprehensive, it differs in terms of external validity and the target population.

Abrar, et al., (2020) investigated the influence of perceived risk (financial risk, product risk, convenience risk and non-delivery risk) on online impulse buying tendency. 200 copies of questionnaires were distributed online to respondents through Facebook and google groups. The study used correlation and regression for data analysis. The study found that overall perceived risk, financial risk and product risk were found to have a moderately negative association with online impulse buying tendency whereas convenience risk and non-delivery risk had negative but weaker association with online impulse buying tendency. Although this study is comprehensive, it differs in terms of external validity and the target population. Another criticism of the study relates to the disparity in analytical methods, as the present research employs PLS-SEM as opposed to another approach.

Azrin, et al. (2024) investigated the impact of security risk, perceived price and online trust on online travel product purchase intentions among Malaysians. This research employs a quantitative correlational design, utilising measurement instruments that have been rigorously developed and validated in prior research. The independent variables (perceived price, online trust, and security risk) were adopted from Phan Tan and Le (2023); Rishi and Khasawneh, (2017); Aggarwal and Rahul (2018), respectively. The dependent variable, online purchase intention, was measured using a scale developed by Rishi and Khasawneh (2017). This research involved a convenience sample of the public in Malaysia. Based on Krejcie and Morgan's (1970) table, a sample size of 384 participants was deemed sufficient for data analysis. To achieve this, self-administered Google Forms were distributed to approximately 400 participants, with additional questionnaires provided to mitigate potential low response rates. In addition to the correlation analysis, the researchers conducted a regression analysis to examine whether the three independent variables (perceived price, online trust, and security) significantly influence or contribute to online purchase intention. The analysis reveals that while all independent variables exhibit a significant relationship with online purchase intention, only online trust shows a positive significant correlation. In contrast, security risk, and perceived price are negatively associated with online purchase intention. Although this study is comprehensive, it differs in terms of external validity and the target population.

Handoyo (2024) conducted a comprehensive meta-analysis investigates the significant factors influencing consumer decision-making in e-commerce. Predominantly focusing on the parameters of trust, perceived risk, perceived security risk, and electronic word-of-mouth (e-WOM), this study provides insightful

revelations on their integral roles in shaping e-commerce purchasing decisions. The findings demonstrate that trust, perceived risk, perceived security risk, and e-WOM significantly influence consumers' e-commerce purchasing decisions. Perceived Risk plays a substantial moderating role in the relationship between Trust and e-commerce purchasing decisions, amplifying the importance of managing and minimizing risk in online transactions to cultivate consumer trust. Contrastingly, the roles of Perceived Security and e-WOM do not hold the same moderating effect on the trust-purchasing decision nexus, underscoring the direct yet unmoderated influence these factors have on e-commerce purchasing behaviors. Furthermore, the research reveals no significant size effect difference among respondents from high-income and low-income countries or between general internet users and online shoppers concerning the impact of trust on e-commerce purchasing decisions. This intriguing finding suggests the universal importance of trust in the digital purchasing landscape, irrespective of socio-economic status or the degree of e-commerce engagement. This study is comprehensive; however, it differs in terms of methodology as the current study is survey research.

**The Perceived Risk Theory (PRT)**

The Perceived Risk Theory (PRT), introduced by economist Raymond A. Bauer in 1960, explains how consumers make decisions under uncertainty by evaluating potential risks associated with purchases. While initially developed for traditional retail settings, the theory has evolved to encompass digital commerce environments, where online transactions present distinct risks compared to physical shopping. These perceived risks in e-commerce encompass multiple dimensions, including financial, product, security, privacy, and performance risks, which collectively influence consumers' purchase intentions and decision-making behavior (Bauer, 1960; Featherman & Pavlou, 2003).

According to PRT, consumers engage in active assessment of potential negative outcomes before finalizing a purchase decision, with their perceived level of risk directly influencing their behavior. This assessment encompasses multiple risk dimensions that combine to form an overall risk perception, ultimately determining whether a consumer proceeds with or abandons a purchase. The digital nature of online shopping amplifies these risk perceptions since consumers cannot physically examine products before purchase, leading to increased concerns about potential losses and disappointment (Featherman & Pavlou, 2003).

When applied to understanding "The Effect of Perceived Risk on Consumer Online Purchase Intentions," PRT illuminates how various risk dimensions affect consumers' willingness to make online purchases. The theory suggests that elevated risk perceptions often lead consumers to abandon online shopping carts or avoid certain e-commerce platforms entirely, demonstrating the direct relationship between perceived risk and purchase intentions. However, e-commerce platforms can positively influence purchase intentions by implementing risk mitigation strategies, such as enhanced security measures and transparent return policies (Pavlou, 2003; Kim et al., 2008).

## METHODOLOGY

This study adopted a survey research design to collect and analyze data from a diverse sample of participants relevant to the research topic. This design is valuable as it ensures broad coverage and representation of the target population, providing a comprehensive understanding of the research problem.

The study's population consists of individuals residing in Abuja, the Federal Capital Territory (FCT), who have internet access and have either made online purchases or expressed interest in online shopping within the past year. As a result, while the population is finite, its exact size is indeterminable.

To determine an appropriate sample size, Cochran's (1963) formula for an infinite population was applied. This formula accounts for the desired confidence level, margin of error, and estimated proportion, allowing for the calculation of a sample size that accurately represents the population.

The formula is:

$$n = \frac{Z^2 \times p \times q}{E^2}$$

where:
n is the sample size
Z is the Z-score for the desired level of confidence (e.g., 1.96 for a 95% confidence level)
p is the estimated proportion of the population with the characteristic of interest
q is 1 - p (the proportion of the population without the characteristic of interest)
E is the desired margin of error (expressed as a decimal)
Thus, the sample size for this study is:

$$n = \frac{1{,}96^2 \times 0.5 \times 0.5}{0.05^2} = 385$$

The study recommends a minimum sample size of 385 respondents. In line with Israel's (2013) guidance, an additional 10%–30% should be included to account for potential non-responses or unreturned questionnaires. Accordingly, 10% of the sample size, equivalent to 39 respondents, was added, resulting in a total of 425 questionnaires for distribution. Respondents were selected using a combination of purposive and convenience sampling techniques. Data for this study was collected from primary sources through a structured questionnaire. The questionnaire employed a five-point Likert scale, with response options ranging from "strongly agree" to "strongly disagree."

**Construct Reliability**

To effectively establish the reliability of the concept, it is generally accepted that both Cronbach's alpha and composite reliability (CR) should exceed the threshold of 0.7, which is widely regarded as the standard for ensuring a strong level of internal consistency. Table 3.1 presents the results for Cronbach's Alpha, rho_A, composite reliability, and average variance extracted.

**Table 3.1: Construct Reliability and Validity of the Indicators**

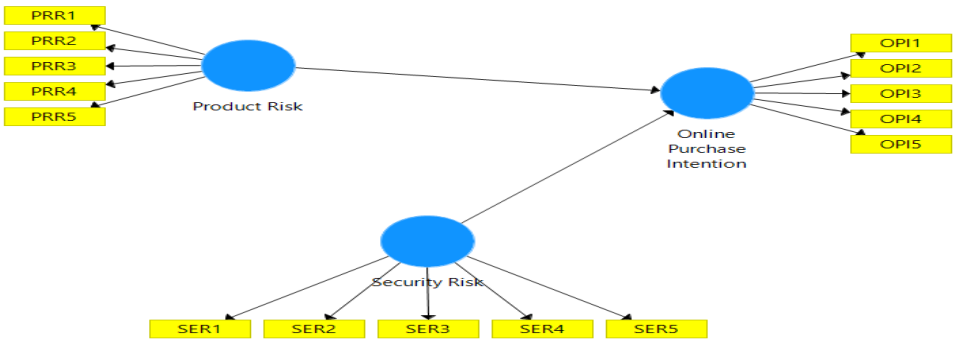
| Variables | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) |
|---|---|---|---|---|
| Product Risk | 0.833 | 0.816 | 0.838 | 0.697 |
| Security Risk | 0.817 | 0.825 | 0.876 | 0.676 |
| Online Purchase Intention | 0.854 | 0.871 | 0.882 | 0.665 |

**Source*:* Researcher's Computation using SMART PLS.**

Table 3.1 presents the construct reliability and validity of the indicators, assessed through Cronbach's Alpha, rho_A, Composite Reliability (CR), and Average Variance Extracted (AVE). Cronbach's Alpha values for all constructs—Product Risk (0.833), Security Risk (0.817), and Online Purchase Intention (0.854)—exceed the commonly accepted threshold of 0.7, indicating strong internal consistency reliability. Similarly, the rho_A values, which provide an alternative measure of reliability, fall within an acceptable range, further supporting the constructs' reliability. Composite Reliability (CR) values for Product Risk (0.838), Security Risk (0.876), and Online Purchase Intention (0.882) all surpass the recommended minimum threshold of 0.7, confirming the reliability of the measurement model. Additionally, the Average Variance Extracted (AVE) for all constructs—Product Risk (0.697), Security Risk (0.676), and Online Purchase Intention (0.665)—exceed the minimum benchmark of 0.5. This confirms that a substantial proportion of the variance in each construct is explained by its respective indicators, thereby establishing convergent validity.

The study employed Partial Least Square Structural Equation Modeling (PLS-SEM) to examine the effect of each independent variable on the dependent variable. Smart PLS was used to code and analyze the data for this study to achieve all the set objectives.

**Structural Model**




## RESULT AND DISCUSSION

### Data Presentation

**Table 4.1: Distribution and Retrieval of Questionnaire**

| Questionnaires | Frequency | Percent (%) |
|---|---|---|
| Returned | 391 | 92 |
| Not returned | 34 | 8 |
| **Total** | **425** | **100** |

**Source: Field Survey, 2024**

Table 4.1 presents a detailed summary of the questionnaire distribution and response rate. Out of the total questionnaires distributed, 391 were successfully retrieved, representing 92% of the total sample. In contrast, 34 questionnaires were not returned, accounting for 8% of the total distributed. The high response rate of 92% reflects an effective data collection process, demonstrating strong participant engagement and cooperation. This substantial response rate enhances the reliability and representativeness of the study's findings by minimizing potential non-response bias. With a total of 425 questionnaires distributed, the study ensures a robust sample size for comprehensive data analysis.

### Descriptive Statistics

**Table 4.2: Descriptive Statistics**

| Statistic | PRR | SER | OPI |
|---|---|---|---|
| **Mean** | 3.224 | 2.958 | 3.102 |
| **Median** | 2.545 | 3.103 | 2.123 |
| **Maximum** | 5.000 | 5.000 | 5.000 |
| **Minimum** | 1.000 | 1.000 | 1.000 |
| **Std. Dev.** | 1.231 | 1.223 | 1.113 |
| **Skewness** | 0.121 | -2.631 | 0.212 |
| **Excess Kurtosis** | 3.010 | 3.219 | 4.010 |

*Source: Researcher's Computations from Smart PLS*

Table 4.2 presents the descriptive statistics for Product Risk (PRR), Security Risk (SER), and Online Purchase Intention (OPI), assessing key measures such as mean, median, standard deviation, skewness, and kurtosis in relation to established thresholds. The mean values for PRR (3.224), SER (2.958), and OPI (3.102) suggest that respondents generally provided moderate ratings on the measurement scale. The median values—PRR (2.545), SER (3.103), and OPI (2.123)—indicate a slight variation in the central tendency, with SER having a median slightly above its mean, suggesting a negatively skewed distribution. The standard deviation values for PRR (1.231), SER (1.223), and OPI (1.113) all fall within the acceptable range (below 1.5), indicating moderate dispersion and consistency in responses.

Skewness values reveal the symmetry of the data distribution, with PRR (0.121) and OPI (0.212) exhibiting slight positive skewness, meaning responses are moderately concentrated toward lower values.

Both values fall within the acceptable threshold of -1 to +1, indicating an approximately normal distribution. However, SER (-2.631) shows a strong negative skewness, exceeding the acceptable limit, suggesting that most respondents perceived security risk to be low. Kurtosis values provide insight into the shape of the data distribution. A normal distribution typically has a kurtosis value of 3. PRR (3.010) and SER (3.219) are slightly above this threshold, indicating moderate peakedness, while OPI (4.010) is more leptokurtic, suggesting a higher concentration of responses around the mean with fewer extreme values.

**Table 4.3: Loading factors item**

| Latent Variable | Manifest Variable | Loading | t-statistic |
|---|---|---|---|
| Product Risk (PRR) | PRR 1 | 0.878 | 28.311 |
| | PRR2 | 0.798 | 24.061 |
| | PRR3 | 0.892 | 47.246 |
| | PRR4 | 0.785 | 44.116 |
| | PRR5 | 0.902 | 44.534 |
| Security Risk (SER) | SER1 | 0.932 | 29.742 |
| | SER2 | 0.875 | 24.027 |
| | SER3 | 0.879 | 23.004 |
| | SER4 | 0.924 | 17.423 |
| | SER5 | 0.933 | 17.301 |
| Online Purchase Intention (OPI) | OPI1 | 0.904 | 17.112 |
| | OPI2 | 0.921 | 16.923 |
| | OPI3 | 0.914 | 18.734 |
| | OPI4 | 0.932 | 19.545 |
| | OPI5 | 0.893 | 20.356 |

**Source: Researcher's Computations from Smart PLS**

Table 4.3 presents the factor loadings and t-statistics for the manifest variables of Product Risk (PRR), Security Risk (SER), and Online Purchase Intention (OPI). Factor loadings measure the strength of the relationship between latent variables and their corresponding indicators, with higher values indicating stronger associations. A commonly accepted threshold for factor loadings is 0.70, with loadings above this level considered acceptable for establishing construct validity. Additionally, t-statistics above 1.96 indicate statistical significance at the 5% level, ensuring that the loadings are reliable.

For Product Risk (PRR), all factor loadings exceed the 0.70 threshold, ranging from 0.785 (PRR4) to 0.902 (PRR5), demonstrating strong convergent validity. The associated t-statistics, ranging from 24.061 to 47.246, confirm statistical significance, reinforcing the reliability of these indicators in measuring product risk. Similarly, Security Risk (SER) exhibits strong factor loadings, with values ranging from 0.875 (SER2) to 0.933 (SER5), all exceeding the 0.70 benchmark. The t-statistics, though lower than those of PRR, remain well above the critical value of 1.96, ranging from 17.301 to 29.742. This suggests that the selected manifest variables effectively capture the construct of security risk. For Online Purchase Intention (OPI), factor loadings are consistently high, ranging from 0.893 (OPI5) to 0.932 (OPI4), further demonstrating strong construct validity. The t-statistics, ranging from 16.923 to 20.356, exceed the threshold of 1.96, confirming that these indicators significantly contribute to the measurement of online purchase intention.

**Figure 4.1: PLS Algorithm (item loading, path coefficient and $R^2$**

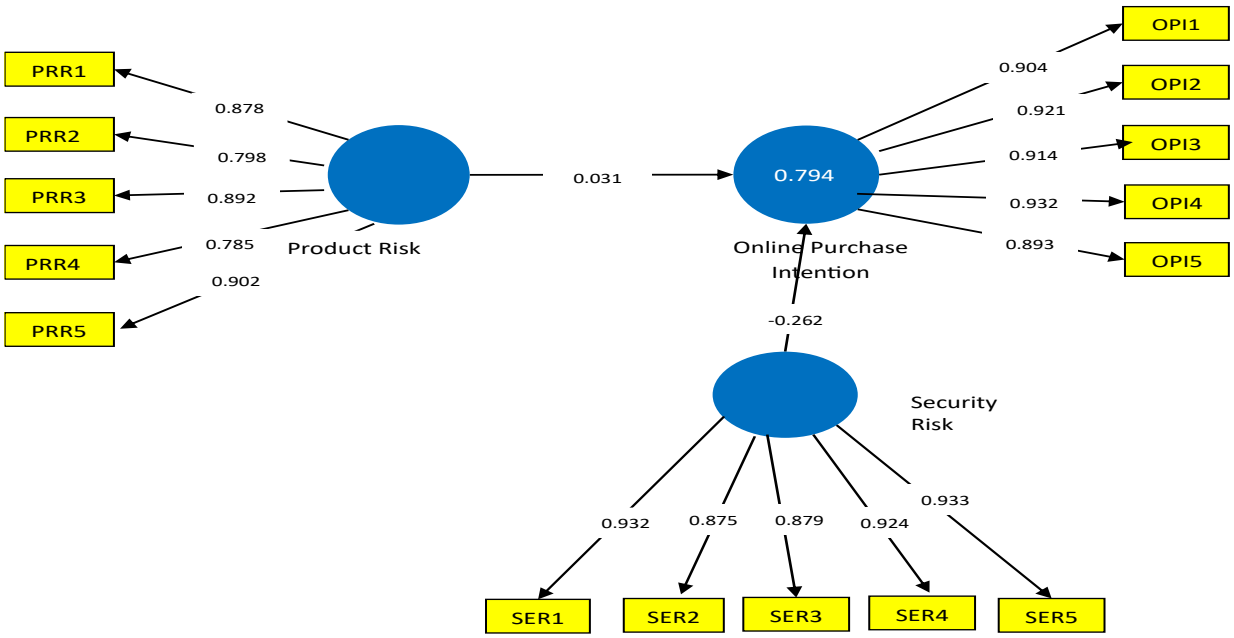



Figure 4.1 illustrates that the independent variables—Product Risk and Security Risk—serve as significant predictors of online purchase intention. The statistical significance of these risk factors is demonstrated by the corresponding t-values and probability values obtained from the analysis. Additionally, a detailed assessment of these latent variables necessitates the use of component scores assigned to each variable within the measurement scales. To facilitate hypothesis testing, it is essential to establish relationships between the latent variables, particularly examining the expected influence of these risk factors on the dependent variable. Analyzing these relationships in depth provides valuable insights into the collective impact of product and security risks on consumers' online purchase intentions.

## Hypotheses Testing

**Table 4.4: Path Coefficient of the Model for Hypotheses Testing**

| Hypothesis | Beta | t-value | p-value | Decision | $f^2$ |
|---|---|---|---|---|---|
| $H_{o1}$: Product Risk → Online Purchase Intention | 0.031 | 1.421 | 0.342 | Accept Ho | 0.002 |
| $H_{o2}$: Security Risk → Online Purchase Intention | -0.262* | -3.434 | 0.021 | Rejected Ho | 0.121 |

**Source: Researcher's Computation from Smart-PLS 3 2024**

### Hypothesis One

**$H0_1$:** product risk has no significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT

Table 4.4 presents the path coefficient results for testing the relationship between Product Risk and Online Purchase Intention. The beta coefficient (β = 0.031) indicates a weak and positive relationship between Product Risk and Online Purchase Intention. However, the statistical significance of this relationship is evaluated using the t-value and p-value. A commonly accepted threshold for significance requires a t-value greater than 1.96 and a p-value less than 0.05 for a hypothesis to be rejected at the 5% significance level. In this case, the t-value of 1.421 is below the required threshold, and the p-value of 0.342 exceeds the 0.05 benchmark. This implies that Product Risk does not have a statistically significant effect on Online Purchase Intention. As a result, the null hypothesis ($Ho_1$) is accepted, meaning there is no sufficient evidence to conclude that Product Risk significantly influences consumers' intent to make online purchases. Additionally, the effect size ($f^2$ = 0.002) is extremely small, further reinforcing the minimal impact of Product Risk on Online Purchase Intention. According to Cohen's (1988) guidelines,

effect sizes of 0.02, 0.15, and 0.35 correspond to small, medium, and large effects, respectively. The value of 0.002 falls far below the threshold for even a small effect, confirming that Product Risk has a negligible influence on Online Purchase Intention.

**Hypothesis Two**

**$H0_2$:** security risk has no significant effect on consumer online purchase intentions in the e-commerce industry in Abuja FCT

Table 4.4 presents the path coefficient results for testing the relationship between Security Risk and Online Purchase Intention. The beta coefficient ($\beta$ = -0.262) indicates a negative relationship between Security Risk and Online Purchase Intention, suggesting that higher perceived security risks are associated with lower online purchase intention. For statistical significance, a hypothesis is rejected if the t-value exceeds 1.96 and the p-value is below 0.05 at the 5% significance level. In this case, the t-value of -3.434 is well above the required threshold (in absolute terms), and the p-value of 0.021 is below 0.05. These results confirm that Security Risk has a statistically significant negative effect on Online Purchase Intention, leading to the rejection of the null hypothesis ($Ho_2$). Furthermore, the effect size ($f^2$ = 0.121) suggests a small to moderate impact of Security Risk on Online Purchase Intention, based on Cohen's (1988) effect size interpretation (0.02 = small, 0.15 = medium, 0.35 = large). This indicates that while Security Risk plays a notable role in shaping consumers' willingness to make online purchases, other factors may also contribute significantly.

**Table 4.5: $R^2$ of the Model**

| Dependent Variable | $R^2$ |
|---|---|
| Online Purchase Intention | 0.794 |

**Source: Researcher's Computation from Smart-PLS 3**

Table 4.5 presents the coefficient of determination ($R^2$) for the model, which measures the extent to which the independent variables explain the variation in the dependent variable, Online Purchase Intention. In this study, the $R^2$ value of 0.794 indicates that 79.4% of the variance in Online Purchase Intention is explained by the independent variables included in the model (Product Risk and Security Risk). This suggests a strong explanatory power, as higher $R^2$ values (closer to 1) indicate a better fit of the model. According to Chin (1998), $R^2$ values of 0.67, 0.33, and 0.19 can be categorized as substantial, moderate, and weak, respectively. Based on this benchmark, an $R^2$ of 0.794 demonstrates a substantial model fit, meaning that the predictors effectively account for a large portion of the variation in Online Purchase Intention. However, while this indicates that Product Risk and Security Risk play a key role in influencing Online Purchase Intention, the remaining 20.6% of the variance is influenced by other factors not included in the model. Future research may explore additional determinants—such as trust, perceived ease of use, or brand reputation—to further enhance the model's predictive power.

**Discussion of Findings**

**Product risk and consumer online purchase intentions in the e-commerce industry in Abuja FCT**

The first objective of this study was to examine the effect of product risk on consumer online purchase intentions in the e-commerce industry in Abuja FCT. The result showed that product risk has a positive but statistically insignificant effect on online purchase intention in the e-commerce industry in Abuja FCT.

This suggests that while consumers may acknowledge potential risks associated with product quality, description accuracy, or functionality, these concerns do not play a decisive role in their purchasing decisions. A possible explanation for this could be the presence of trust-building mechanisms such as customer reviews, return policies, and brand reputation, which mitigate the perceived impact of product risk. For e-commerce businesses, this implies that while ensuring product quality remains important, addressing other factors—such as enhancing security measures and improving customer experience—may have a more substantial impact on driving online purchase intentions. Retailers should continue to

provide detailed product descriptions, high-quality images, and customer feedback to further reassure buyers. However, greater emphasis should be placed on improving security frameworks, payment protection, and trust-building strategies, as these factors might have a stronger influence on consumer behavior. Additionally, policymakers and industry stakeholders can leverage this insight to develop regulatory frameworks that enhance consumer protection while fostering an environment that promotes trust and confidence in online shopping. Future research could further explore other psychological and contextual factors that might interact with product risk perceptions to influence consumer decisions.

The finding of this study aligns with that of Abdullahi et al. (2023), Mayo and Layante (2022) who examined the effect of perceived risk dimensions on online buying behaviour and found a positive and insignificant effect of product risk on consumers' purchase intention. It however contradicts the result of Abrar, et al., (2020) who investigated the influence of perceived risk (financial risk, product risk, convenience risk and non-delivery risk) on online impulse buying tendency and found product risk to have a moderately negative association with online impulse buying tendency.

**Security risk and consumer online purchase intentions in the e-commerce industry in Abuja FCT**

In the second objective, this study examined the effect of security risk on consumer online purchase intentions in the e-commerce industry in Abuja FCT. The findings indicate that security risk has a negative and statistically significant effect on online purchase intention in the e-commerce industry in Abuja FCT.

This suggests that consumers are highly concerned about the safety of their personal and financial information when engaging in online transactions. Issues such as data breaches, fraudulent activities, identity theft, and lack of secure payment gateways likely deter potential buyers from making purchases. For e-commerce businesses, this underscores the critical importance of enhancing cybersecurity measures and building consumer trust in online transactions. Implementing robust encryption technologies, multi-factor authentication, secure payment systems, and transparent privacy policies can help alleviate security concerns and encourage more consumers to engage in online shopping. Additionally, offering buyer protection programs, fraud detection mechanisms, and clear refund policies can further reassure customers and boost their confidence in using e-commerce platforms. From a policy perspective, regulatory bodies should strengthen cybersecurity laws and enforce compliance with data protection regulations to create a safer e-commerce environment. Consumer education on safe online shopping practices—such as recognizing phishing scams, verifying website authenticity, and using secure payment methods—can also play a crucial role in mitigating security risks.

The findings that security risk has a negative and statistically significant effect on online purchase intention in the e-commerce industry in Abuja FCT aligns with that of Azrin, et al. (2024) who investigated the impact of security risk, perceived price and online trust on online travel product purchase intentions among Malaysians and Handoyo (2024) who conducted a comprehensive meta-analysis investigates the significant factors influencing consumer decision-making in e-commerce and their results showed a negative and statistically significant effect of security risk on online purchase intention.

## CONCLUSION AND RECOMMENDATIONS

This study examined the effect of risk perception (product risk and security risk) on online purchase intention in the e-commerce industry in Abuja, FCT. The findings revealed that product risk has a positive but statistically insignificant effect on consumers' online purchase intentions. This suggests that while concerns about product quality and description accuracy exist, they do not significantly deter consumers from making online purchases, possibly due to the presence of trust-enhancing mechanisms such as reviews, return policies, and brand reputation. Conversely, security risk was found to have a negative and statistically significant impact on online purchase intention, indicating that consumers are highly sensitive to issues related to data privacy, fraud, and payment security. The fear of financial loss and identity theft discourages consumers from engaging in online shopping, highlighting the need for

improved cybersecurity measures and trust-building strategies. Overall, the study concludes that risk perception has a significant effect on online purchase intentions in Abuja, FCT.

Based on the empirical findings of this study, the following recommendations are suggested:

i. E-commerce businesses should invest in advanced cybersecurity measures such as SSL encryption, multi-factor authentication, and fraud detection systems. Implementing secure payment gateways and providing clear consumer protection policies will help build trust and encourage more online transactions.
ii. Businesses should still enhance product transparency and consumer trust by providing detailed product descriptions, high-resolution images, and authentic customer reviews. Offering hassle-free return policies and warranties can further reassure customers and reduce hesitation in making online purchases.

**References**

Abdullah, M., & Kumar, S. (2021). Understanding consumer risk perception in digital markets: A multi-dimensional approach. *Journal of Consumer Psychology*, 33(4), 278-295.

Abdullahi, W.G., Babangida, S.Z., Abdullahi, F.M., Abubakar, Z., & Ahmad, A.Y. (2023). Effect Of Perceived Risk on Online Buying Behavior Among Undergraduate Students in Ahmadu Bello (Abu) University Zaria. *Gusau Journal of Economics and Development Studies* (GUJEDS) Vol. 3(1).

Abrar, K., Naveed, M., & Ramay, M. I. (2020). Impact of perceived risk on online impulse buying tendency: an empirical study in the consumer market of Pakistan. *Journal of Accounting & Marketing*, 6(3), 2–6. https://doi.org/10.4172/2168- 9601.1000246.

African Development Bank. (2023). Digital commerce and financial inclusion in Africa: Annual report 2023. African Development Bank Publications.

Anderson, P., Williams, R., & Thompson, K. (2022). Global e-commerce risk perception and consumer behavior: A meta-analysis. *Journal of Electronic Commerce Research*, 23(4), 156-178.

Azrin, A.R., Sharfika, R., Aervina, M., Norsafriman, R. (2024). Perceived Price, Online Trust, and Security Risk: Decoding Online Travel Product Purchase Intention through the Perceived Risk Model. *International Journal of Academic Research in Business and Social Sciences* Vol. 14, No. 9, 2024, E-ISSN: 2222-6990.

Chen, S., & Zhou, M. (2023). Consumer transaction security concerns in online shopping: The mediating role of trust. *International Journal of Information Management*, 63, 102485.

Cohen, M., Johnson, E., & Parker, G. (2021). Trust and privacy concerns in smart products: A consumer perspective. *Journal of Marketing*, 85(4), 121-145.

European Consumer Report. (2023). Digital market trends and consumer confidence in the EU. European Commission Publishing.

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon* 10 (2024) e29714.

Ibrahim, M., & Nnamdi, O. (2023). E-commerce adoption patterns in Nigeria's capital territory: A study of risk perception among urban consumers. *Nigerian Journal of Business Studies*, 15(2), 45-63.

Lee, J., & Kim, S. (2022). Algorithmic bias and product risk: A framework for AI-enabled product development. *Management Science*, 68(5), 3456-3478.

Lin, H., & Fang, J. (2023). Impact of transaction security on online consumer trust and purchase intention. *E-Commerce and Consumer Behavior*, 12(2), 121-137.

Mayo, J.A., & Layante, J.P. (2022). Perceived risk and online purchase intention of selected public-school teachers: A study in Calapan City, Oriental Mindoro, Philippines. *World Journal of Advanced Research and Reviews,*16(02), 908–925.

Mitchell, V., & Harris, P. (2022). Consumer risk perception and online shopping behavior: A theoretical framework. *International Journal of Electronic Commerce Studies*, 15(2), 145-163.

Mohammed, A., & Okonkwo, C. (2022). Understanding e-commerce barriers in emerging African markets: A multi-country analysis. *African Journal of Marketing Management*, 14(3), 89-107.

Nigerian Bureau of Statistics. (2023). Digital economy report: E-commerce growth and trends in Nigeria. Federal Government of Nigeria.

Park, J., Lee, S., & Brown, M. (2022). Understanding online consumer behavior: A study of purchase intentions in e-commerce. *Journal of Business Research*, 128, 356-373.

Smith, J., & Jones, M. (2023). Global e-commerce market analysis: Trends and projections 2021-2026. *International Journal of Digital Commerce*, 18(2), 234-251.

Wang, Y., & Chang, L. (2023). Determinants of online purchase intentions: An integrated model. *Internet Research*, 33(1), 67-84.

Watson, R., & Lee, S. (2023). Cybersecurity threats in global e-commerce: Assessment and implications. *Journal of Internet Security*, 12(4), 312-329.

Zhang, L., & Thompson, R. (2023). The psychology of risk perception in e-commerce: An integrated model. *Journal of Risk Research*, 26(3), 412-429.

Zhang, L., & Wang, R. (2019). Digital transformation and product risk: A cybersecurity perspective. *Journal of Operations Management*, 65(4), 678-701.