

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control



Nguyen, Hong Tam¹, Nguyen, Anh Vu², Tran, Phuong Thao³, Mai, Hong Nhung⁴,
Pham, Thi Van Anh⁵

¹Hai Ba Trung District, Ha Noi Capital, Viet Nam

²Hai Ba Trung District, Ha Noi, Viet Nam

³Dong Da District, Ha Noi, Viet Nam

⁴Hai Ba Trung District, Ha Noi, Viet Nam

⁵Hoang Mai District, Ha Noi, Vietnam

ABSTRACT: This study explores the impact of Cyber-fraud Perception (CFP) on E-commerce Purchase Behavior (PBE), with a focus on the mediating role of Perceived Behavioral Control (PBC). Using a survey method, data were collected through questionnaire surveys, yielding 364 valid responses. Structural equation modeling (SEM) with 5,000 bootstrapping iterations was used to test the proposed hypotheses. The findings reveal that Cyber-fraud Perception directly and positively influences both Perceived Behavioral Control and E-commerce Purchase Behavior. Additionally, Perceived Behavioral Control acts as a mediator in the relationship between Cyber-fraud Perception and E-commerce Purchase Behavior. The research has contributed some theoretical and practical implications for e-commerce businesses.

KEYWORDS: Purchase behavior; e-commerce; perception

1. INTRODUCTION

The rapid growth of e-commerce has revolutionized consumer shopping behavior, offering convenience, variety, and accessibility. However, with this digital transformation, concerns related to cyber fraud have emerged, influencing consumer trust and decision-making in online purchases ([Wahab et al., 2023](#)). Cyber-fraud perception plays a crucial role in shaping consumer attitudes, as individuals who perceive higher risks in online transactions may exhibit hesitation or avoidance in purchasing behavior ([Hansen et al., 2018](#)).

One key factor that can mitigate or amplify the impact of cyber-fraud perception on purchase behavior is **Perceived Behavioral Control (PBC)**. Rooted in the **Theory of Planned Behavior (TPB)** ([Ajzen, 1991](#)), PBC refers to an individual's belief in their ability to control their behavior in a given context. In e-commerce, consumers with high perceived control over online transactions (e.g., secure payment options, refund policies, and digital literacy) may be less deterred by cyber-fraud concerns and more willing to proceed with purchases ([Gefen et al., 2003](#)).

This study aims to investigate the relationship between **cyber-fraud perception and purchase behavior on e-commerce platforms**, with **Perceived Behavioral Control** as a mediating factor. Specifically, we examine (1) the direct impact of cyber-fraud perception on consumer purchase behavior, (2) the role of PBC in influencing purchasing decisions, and (3) whether PBC mitigates the negative impact of cyber-fraud perception on online shopping.

By exploring these relationships, this research contributes to the growing literature on digital consumer behavior and provides insights for e-commerce platforms to enhance user confidence and transaction security. The findings will help businesses understand how to design safer and more trustworthy online shopping environments to encourage consumer participation despite concerns about cyber fraud.

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

2. LITERATURE REVIEWS AND HYPOTHESIS DEVELOPMENT

2.1. Basic concepts

2.1.1. Purchase behavior on e-commerce

[Victor et al. \(2023\)](#) defined purchasing behavior on e-commerce as the buying and selling of goods and services through electronic platforms, utilizing information technology to enhance convenience, speed, and accessibility for consumers and businesses. Furthermore, when exploring the concept of consumer purchasing behavior on e-commerce, [Shim et al. \(2013\)](#) posited that it is the process through which consumers engage in the acquisition of products and services via the Internet.

From the above definitions, the research team has drawn the most general concept of purchase behavior on E-commerce (PBE) as the actual performance of purchasing and selling goods or services through e-commerce platforms using technology. This behavior takes place through interactions between consumers and the online environment.

2.1.2. Consumer's cyber-fraud perception

According to [Rookes and Willson \(2005\)](#), from a psychological perspective, perception is a process involving the recognition and interpretation of stimuli, both of which are registered through human sensory organs. Cyber-fraud can be defined as a type of criminal activity involving the unauthorized access and use of individuals' personal information through various means ([Buchanan, 2016](#)). Based on the studies by [Kim et al. \(2008\)](#) and [Warr \(2000\)](#), cyber-fraud perception is an individual's recognition and interpretation of the vulnerability to financial loss when conducting transactions over the Internet.

2.1.3. The TPB theory

The theory of planned behavior (TPB) is a psychological theory that explains how attitude, subjective norms, and perceived behavioral control influence the actual behavior ([Ajzen, 1991](#)). The Theory of Planned Behavior (TPB; [Ajzen, 1991](#)), developed from the Theory of Reasoned Action (TRA; [Ajzen & Fishbein, 1975](#)), posits that a behavior can be predicted or explained by behavioral intentions to perform that behavior.

Ajzen evolved the Theory of Planned Behavior (TPB) by extending the Theory of Reasoned Action (TRA) with the addition of Perceived behavioral control. The perceived behavioral control reflects the ease or difficulty of performing a behavior, which depends on the availability of resources and opportunities to perform the behavior ([Chaturvedi et al., 2020](#); [Thi Tuyet Mai, N. 2019](#)). The TPB model is considered more optimal than the TRA model in predicting and explaining the behavior of information consumers in the same research context and content, thanks to the Perceived behavioral control factor.

2.2. Hypotheses

2.2.1. Cyber-fraud perception and purchase behavior on e-commerce

Cyber fraud perception encompasses understanding various forms of online criminal activities and the measures to protect against them. It includes knowledge of prevalent scams like phishing, email spoofing, and credit card frauds ([Arora, 2024](#)). According to the study by [Narayanan et al. \(2012\)](#), a higher perception of cyber-fraud makes consumers more hesitant to shop online. In Indonesia, increased awareness or experience of online fraud has led to a decline in e-commerce transactions ([Rofiq, A. 2012](#)). Therefore, our proposed hypothesis is:

H1: Cyber-fraud perception positively affects consumers' purchase behavior through e-commerce platforms.

2.2.2. Cyber-fraud perception and perceived behavioral control

Perceptions of cyber fraud can significantly influence an individual's perceived behavioral control (PBC), which refers to one's belief in their capability to perform a specific behavior. According to the Theory of Planned Behavior (TPB) ([Ajzen, 1991](#)), PBC is a critical determinant of behavioral intentions and actions. When individuals perceive a high risk of cyber fraud, they may feel less confident in their ability to engage safely in online activities, leading to decreased PBC. This diminished sense of control can result in avoidance behaviors, such as refraining from online transactions or limiting internet usage. A study by [Liang and Xue \(2010\)](#) found that heightened awareness of cyber threats lowers perceived control unless accompanied by effective coping strategies. In this research, the following research hypothesis is considered:

H2: Cyber-fraud perception positively affects perceived behavioral control

2.2.3. Perceived behavioral control

Perceived behavioral control is considered an important aspect for consumers when considering attitudes toward certain behaviors and the reference group of others in society ([Sun, Law, & Schuckert, 2020](#)). Perceived behavioral control refers to the potential limitations of intentional actions, such as available resources and opportunities. Therefore, perceived behavioral control refers to an

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

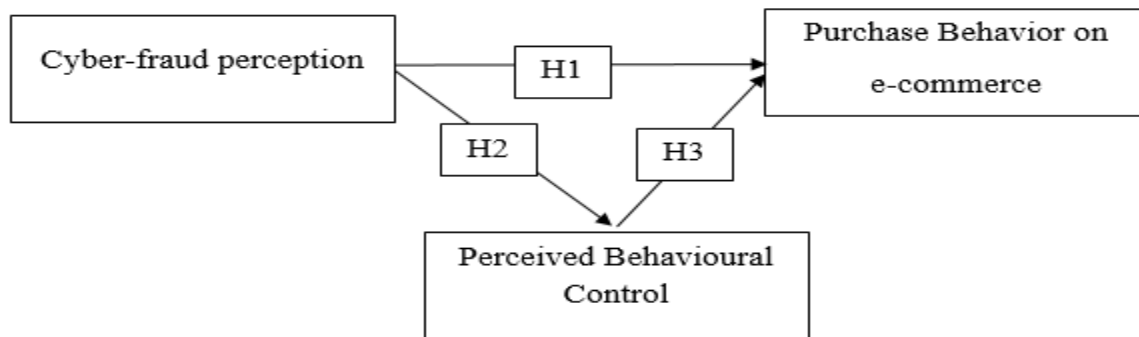
individual's ability to control a certain behavior ([Hsu and Huang, 2012](#)). According to [Tasya et al. \(2024\)](#), perceived behavioral control significantly affects purchase intention. This suggests that when consumers feel they have control over their purchase decisions, they are more likely to have purchase intentions. The study by [Bangun, C., et al \(2023\)](#) showed that perceived behavioral control, subjective norms, attitudes, and perceived values significantly influence purchase intentions and purchase behavior when shopping online. In addition, [Heptariza, A., \(2020\)](#) confirmed that perceived behavioral control has a positive impact on online purchase intentions, which in turn positively influences actual purchase behavior. According to the above studies, perceived behavioral control has a positive impact on behavior either directly or through intention. In this study, the following research hypothesis is considered:

H3: Perceived behavioral control positively affects consumers' purchase behavior through e-commerce platforms

2.2.4. Mediator effect

According to TPB, external factors not only have a direct impact but also indirectly affect consumer behavior through the mediation of PBC ([Ajzen, 1991](#)). Ajzen's initial research on the Theory of Planned Behavior has been applied to investigate the direct effect of perceived behavioral control on intended and actual behavior. Furthermore, the research team also found that perceived behavioral control and factors related to the perception of online fraud are closely linked based on the intrinsic element of perceived behavioral control demonstrated in the TPB model and self-efficacy studies ([Bandura, A 1977](#)). This implies that the perception of online fraud directly affects behavioral control. Therefore, the hypothesis is proposed:

H4: Perceived behavioral control mediates the relationship between cyber fraud perception and e-commerce purchase behavior



Figure_1: The concept model

3. METHODOLOGY

3.1. Sampling and data collection

The authors and participants completely agreed that all information provided in the survey would remain anonymous and entirely voluntary, with the results used exclusively for research purposes. Prior to conducting the survey, key concepts, including vulnerabilities in skills and knowledge, were clearly defined. The data for this study were collected through online surveys conducted in Vietnam in October 2024. The questionnaire was disseminated across multiple online shopping communities on platforms such as Facebook, Zalo, Instagram, Shopee, and TikTok. Before participating, all respondents were explicitly informed that their responses would be used solely for research purposes.

A total of approximately 380 individuals participated in the survey, resulting in 364 valid responses. The demographic characteristics of the respondents are presented in Table 1. Descriptive statistical analysis indicates that female participants accounted for 57.69% of the total sample, while male participants constituted 42.31%. Regarding age distribution, respondents were categorized into four groups: under 18 years old (26.92%), 18–25 years old (24.73%), 26–35 years old (26.10%), and over 36 years old (22.25%). The majority of participants resided in urban areas (57.14%), whereas 42.86% lived in rural areas. In terms of occupation, 48.35% of the respondents were employed, while students and university students accounted for 26.92% and 24.73%, respectively.

Table 1: Demographic Profile of Participants

		Frequency	Percentage (%)
Gender	Male	154	42.308%
	Female	210	57.692%
Age	Under age 18	98	26.923%

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

	Ages 18-25	90	24.725%
	Ages 26-35	95	26.099%
	Over 36	81	22.252%
Living	Urban	208	57.143%
	Countryside	156	42.857%
Occupation	Student	98	26.923%
	University student	90	24.725%
	Working	176	48.352%

Source: Analysis of authors' survey.

3.2. Measures and questionnaire development

To examine the impact of cyber - fraud perceptions in the capability of customers on their purchasing behaviors in e-commerce, our study adopted scales that were developed in previous research. With the variable of cyber fraud perception, we adapted the measurement from a previous study by [\(Im, I et al., 2008\)](#). The perceived behavioral control (PBC) variable was measured using an adapted scale from the study by [\(Crespo and Del Bosque, 2008\)](#). Finally, the measurement of e-commerce purchase behavior (PBE) was adapted from the research of [\(Yadav & Pathak, 2017\)](#) Each variable was scored based on the five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). To avoid common method bias, we translated the Vietnamese version into English, and any differences were resolved before developing the final questionnaire survey. All questions in the survey provided brief explanations to ensure that participants could understand the contexts

3.3. Data analysis

We applied Smart PLS 4 software to conduct the validity and reliability of constructs through Cronbach's Alpha, EFA, CFA.

We evaluated the influence of Cyber - fraud perception on e-commerce purchase behavior by conducting structural equation modeling (SEM). We used the bootstrapping method to examine mediation coefficients. In this research, the bootstrapping sample was 5000 with a confidence interval of 95% and if the confidence interval did not involve zero, the mediations were conducted substantially. We used the Smart PLS 4 of [\(Hair et al., 2017\)](#), which is useful to recognize and estimate the indirect effects [\(Munir et al., 2024\)](#). The results permitted us to express the role of mediating variable (PBC) in the relationship between CBF and PBE.

4. RESULT AND DISCUSSION

4.1. Scale assessment

The evaluation of the model utilizing Smart PLS 4 revealed that the outer loading for the observed variables exceeded 0.7. Consequently, items PBC1 and PBC4 were removed due to their outer loading being below the threshold of 0.7, while the remaining variables met the desired criterion of outer loading greater than 0.7, as presented in **Table 2**. Subsequently, the research team examined the reliability of the scale across the full sample by calculating Cronbach's Alpha. The results indicated that VLS had a Cronbach's Alpha of 0.860, VLK recorded 0.847, PBC achieved 0.856, Uncertainty was at 0.785, and PBE had a value of 0.778. All variables exhibited a Cronbach's Alpha coefficient exceeding 0.7, signifying a good level of reliability for the scale [\(Hair et al., 2010\)](#). Furthermore, Table 2 demonstrates that the EVA coefficient surpassed the acceptable threshold of 0.5, confirming the effectiveness of the structural value. The diagonal values representing discriminant validity were derived from the square of the AVE coefficient, which was greater than the correlations among the dimensions. This indicates that the discriminant validity is robust, as each dimension maintains adequate discrimination, as illustrated in **Table 3**.

Table 2: Measurement model reliability

Variable	Code	Outer loading	VIF	ALpha	CR(rho_c)	AVE
Cyber-fraud perception	CFP1	0.828	1.485	0.738	0.754	0.655
	CFP2	0.749	1.392			
	CFP3	0.847	1.538			
	PBC2	0.883	1.459	0.719	0.719	0.780

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

Perceived Behavior Control	PBC3	0.884	1.459			
Purchase Behavior On E-commerce	PBE1	0.785	1.624	0.737	0.778	0.649
	PBE2	0.767	1.357			
	PBE3	0.861	1.500			

Note: PBC1 and PBC4 were eliminated

Source: authors' survey.

Table 3: Result of the reliability and convergence of the scale

Fornell-Larcker Criterion	CFP	PBC	PBE
Cyber-fraud perception (CFP)	0.809		
Perceived Behavior Control (PBC)	0.222	0.883	
Purchase Behavior On E-commerce (PBE)	0.187	0.197	0.806
Heterotrait-Monotrait Ratio (HTMT)	VLK	PBE	PBC
Cyber-fraud perception (CFP)			
Perceived Behavior Control (PBC)	0.305		
Purchase Behavior On E-commerce (PBE)	0.230	0.263	

Source: Analysis of authors' survey.

4.2. Structural path analysis

The results from the direct path analysis indicate that cyber-fraud perception (CFP) significantly impacts both perceived behavioral control (PBC) and purchase behavior on e-commerce (PBE). Specifically, CFP negatively influences PBC ($\beta = 0.222$, $p = 0.000$), suggesting that higher fraud perception reduces consumers' confidence in their ability to control online purchasing decisions. Similarly, CFP negatively affects PBE ($\beta = 0.151$, $p = 0.007$), implying that consumers with heightened fraud concerns are less likely to engage in online purchases. Meanwhile, PBC positively influences PBE ($\beta = 0.164$, $p = 0.008$), meaning that consumers who feel they have more control over their online shopping decisions are more likely to make purchases. Additionally, the mediation analysis (CFP $\rightarrow$ PBC $\rightarrow$ PBE) shows a marginally significant indirect effect ($\beta = 0.036$, $p = 0.028$), indicating that PBC partially mediates the impact of CFP on PBE. This suggests that while fraud perception directly discourages online shopping, its effect is also channeled through consumers' perceived control over their behavior, reinforcing the idea that enhancing consumer confidence in online purchasing mechanisms may help mitigate the negative effects of fraud perception.

Table 4: Direct Path Analysis

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T	P Values	Result
H2: CFP $\rightarrow$ PBC	0.222	0.226	0.058	3.850	***	Supported
H1: CFP $\rightarrow$ PBE	0.151	0.153	0.057	2.655	***	Supported
H3: PBC $\rightarrow$ PBE	0.164	0.168	0.067	2.440	***	Supported
H4: CFP $\rightarrow$ PBC $\rightarrow$ PBE	0.036	0.038	0.019	1.930	***	Supported

Note: N = 364, *** is $p < 0.001$.

Source: Analysis of authors' survey.

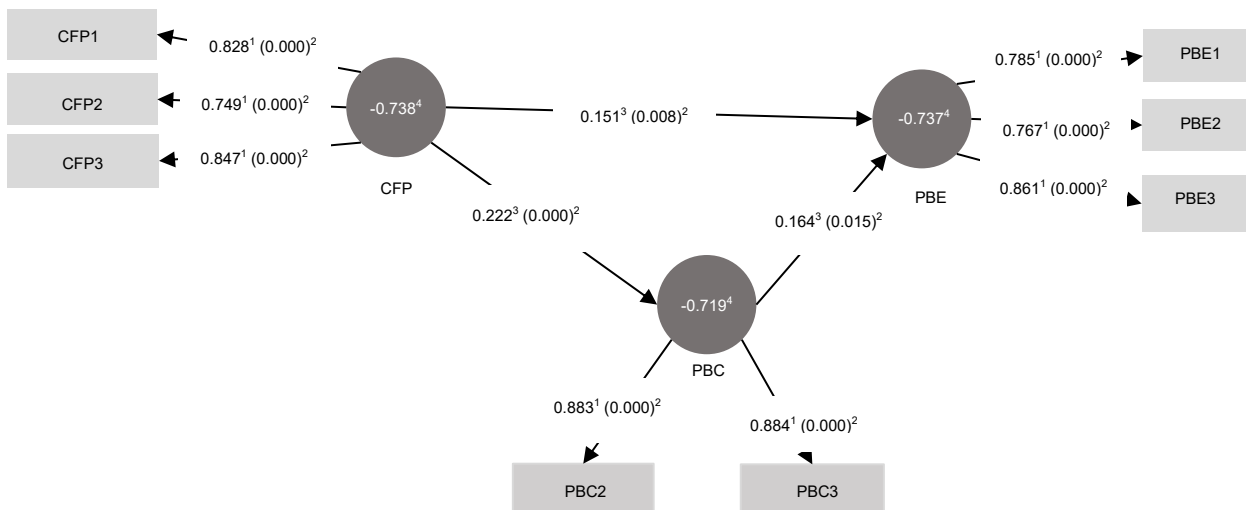
4.3. Discussions

The results of the study showed that CFP has a positive impact on PBE ($O = 0.151$, $p < 0.05$). Although this supports H1, it differs from the prior empirical findings of [Rofiq, A \(2012\)](#). This discrepancy may arise from various factors, including technological and technical advancements in online shopping platforms and the digital space in general. Today, when consumers gain greater awareness of cyber

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

fraud through online information, they tend to increase their purchase behaviors in e-commerce, as they feel more confident in their ability to control their transaction behavior. Furthermore, the study also found that a CFP positively affects PBC ($O = 0.222$, $p < 0.05$). This result, although supporting H2, differs from earlier studies like [Rezk, A et al \(2017\)](#) and [Rofiq, A \(2012\)](#). This difference may be explained by technological factors in the current era. Specifically, when consumers today understand online risks better, they tend to equip themselves with knowledge and skills to control their behavior more effectively. As a result, they gradually feel capable of managing their actions, which increases their perceived behavioral control.

The result also revealed that PBC positively impacts PBE ($O = -0.233$, $p < 0.001$). When compared with prior research, such as [Shufiana, A et al \(2021\)](#), similar results were observed, thereby supporting H3. This means that when individuals feel an increase in their perceived behavioral control, they also feel that they have the resources and ability to manage their transaction behavior, thereby increasing their likelihood of engaging in online purchasing behavior. The study also highlighted that CFP positively affects PBE via PBC ($O = 0.036$, $p < 0.05$). Although this result is consistent with and supports H4, this finding contradicts the prior empirical findings of [Rofiq, A \(2012\)](#). This discrepancy may stem from various factors such as sample size, environment, or even technology. In the context of modern online shopping platforms adopting advanced technological innovations, consumers today develop a more comprehensive understanding of cyber fraud as well as the risks they may encounter when shopping online. This, in turn, enhances their perceived behavioral control, making them more confident in their ability to regulate their shopping process, and ultimately encouraging them to make online purchasing decisions more boldly.



Figure_2. PLS-SEM structural equation modeling results.

Note: ***1: Outer Loading; ***2: P-value; ***3: Path Coefficients; ***4: Cronbach's Alpha

Source: The result from Smart PLS 4.

5. CONCLUSION AND POLICY IMPLICATIONS

5.1. Theoretical and practical implications

From a theoretical perspective, our study contributes to the research on purchasing behavior on e-commerce by examining the intricate relationship between consumers' cyber-fraud perception (CFP), perceived behavioral control (PBC), and purchase behavior in e-commerce (PBE). Specifically, the findings extend the applicability of the Theory of Planned Behavior (TPB) in the context of online transactions, revealing nuanced dynamics that deviate from some previous studies.

From a practical perspective, the findings of our study offer several practical recommendations for e-commerce platforms and consumers to enhance purchasing behavior and the online shopping experience. For e-commerce platforms, the first suggestion is that platforms need to enhance consumer education on online security, helping them better understand risks and how to avoid them. Secondly, user control should be improved by providing tools and features that allow consumers to manage their transactions. Thirdly, optimize the shopping experience to minimize perceived risks, creating a safe and convenient shopping environment. Finally, implement flexible return policies to reduce consumer anxiety. For consumers, the study encourages actively seeking information

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

about products and services from reputable sources. Enhancing digital literacy and online security skills is essential for protecting oneself from risks. Effectively using platform-provided tools, seeking advice from experienced individuals, and adopting smart consumption habits are also crucial factors.

5.2. LIMITATIONS AND FUTURE RESEARCH

- Limitations

This study has several limitations that should be considered when interpreting the findings. The sample size may be limited, restricting the generalizability of the results to a broader population. Additionally, reliance on self-reported data introduces potential biases, such as social desirability and recall errors, which may affect response accuracy. The study also focuses on a specific set of variables, potentially overlooking other significant moderating or mediating factors that could influence the results. Moreover, the context-specific nature of the research may limit its applicability to other industries, regions, or consumer groups, making cross-context comparisons challenging.

- Future research

To address these limitations, future research should expand the sample size and include diverse demographic and geographic groups to improve generalizability. Conducting longitudinal studies would provide deeper insights into behavioral changes over time and enhance causal inferences. Additionally, incorporating new psychological, technological, and socio-economic variables may refine the existing model and uncover additional influencing factors. Cross-cultural comparisons could help identify variations in consumer behavior across different economic and cultural settings. Finally, employing experimental methods or AI-driven behavioral tracking could strengthen the validity of findings and reduce biases associated with self-reported data.

5.3. CONCLUSION

This study contributes to the growing body of literature on consumer behavior in e-commerce by examining the impact of cyber-fraud perception (CFP) on purchase behavior (PBE), with perceived behavioral control (PBC) as a mediating factor. The findings indicate that while CFP negatively affects PBE, PBC plays a crucial role in mitigating this effect, providing consumers with greater confidence in their online transactions. Specifically, the results suggest that when consumers perceive higher risks of cyber fraud, they are less likely to engage in online purchases. However, those who feel they have sufficient control over their purchasing decisions, whether through secure payment options, refund policies, or familiarity with digital platforms, are more likely to proceed with transactions despite concerns about fraud.

From a theoretical perspective, this research extends the Theory of Planned Behavior (TPB) by highlighting the mediating role of perceived behavioral control in the context of online shopping and cybersecurity threats. While previous studies focused on direct relationships between trust and purchasing behavior, our study demonstrates that consumer confidence and self-efficacy in managing online risks are key factors influencing their final purchasing decisions.

From a practical standpoint, the study provides valuable insights for e-commerce platforms and policymakers. Platforms should enhance consumer education on cyber fraud prevention, implement robust security measures, and provide transparent refund policies to boost consumer confidence. Additionally, improving user interfaces with clearer transaction controls and fraud protection features can help mitigate perceived risks, encouraging higher engagement in online shopping. Future research could explore cross-cultural differences in CFP and PBC, as well as the role of emerging technologies such as artificial intelligence in enhancing consumer trust in e-commerce.

REFERENCES

- 1) Ajzen, I. (1991). The Theory of planned behavior. *Organizational Behavior and Human Decision Processes*. <https://doi.org/10.4135/9781446249215.n22>
- 2) Ajzen, I., & Fishbein, M. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.
- 3) Arora, M. S. (2024). Threats, Effects, and Awareness of Cybercrime: A Survey. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*.
- 4) Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84.

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

- 5) Bangun, C. S., Suhara, T., & Husin, H. (2023). The application of theory of planned behavior and perceived value on online purchase behavior. *Technomedia Journal*, 8(1 Special Issues), 123-134.
- 6) Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
- 7) Chaturvedi, P., Kulshreshtha, K., & Tripathi, V. (2020). Investigating the determinants of behavioral intentions of generation Z for recycled clothing: An evidence from a developing economy. *Young Consumers*, 21(4), 403-417.
- 8) Crespo, A. H., & del Bosque, I. R. (2008). The effect of innovativeness on the adoption of B2C e-commerce: A model based on the Theory of Planned Behaviour. *Computers in Human Behavior*, 24(6), 2830-2847.
<https://doi.org/10.1016/j.chb.2008.04.008>
- 9) Gefen, D., Rao, V. S., & Tractinsky, N. (2003, January). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. In *HICSS* (p. 192).
- 10) Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, 1(2), 107-123.
<https://doi.org/10.1504/IJMDA.2017.087624>
- 11) Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate Data Analysis: A Global Perspective*", Pearson Education, London.
- 12) Hansen, J. M., Saridakis, G., & Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, 80, 197-206.
- 13) Heptariza, A. (2020). The effect of attitude, normal subjective and perceived behavioral control (PBC) on actual purchasing through purchases of online purchase in the online retail industry. *Jurnal Ekonomi & Bisnis JAGADITHA*, 7(1), 9-17.
- 14) Hsu, C. H., & Huang, S. (2012). An extension of the theory of planned behavior model for tourists. *Journal of Hospitality & Tourism Research*, 36(3), 390-417.
- 15) Im, I., Kim, Y., & Han, H. J. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & management*, 45(1), 1-9.
- 16) Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544-564.
<https://doi.org/10.1016/j.dss.2007.07.001>
- 17) Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7), 1.
- 18) Model, A. I. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.
- 19) Munir, H., Nauman, S., Ali Shah, F., & Zahid, U. (2024). Attitude towards entrepreneurship education and entrepreneurial intentions among generation Z: unleashing the roles of entrepreneurial self-efficacy and social norms in Pakistani context. *Journal of Entrepreneurship and Public Policy*, 13(2), 255-277. <https://doi.org/10.1108/JEPP-07-2023-0065>
- 20) Narayanan, M., Koo, B., & Cozzarin, B. P. (2012). Fear of fraud and Internet purchasing. *Applied Economics Letters*, 19(16), 1615-1619.
- 21) Rofiq, A. (2012). Impact of cyber fraud and trust of e-commerce system on purchasing intentions: Analysing planned behaviour in Indonesian business (Doctoral dissertation, University of Southern Queensland).
- 22) Rookes, P., & Willson, J. (2005). *Perception: Theory, development and organisation*. Routledge.
- 23) Shim, J. K., Qureshi, A. A., Siegel, J. G., & Siegel, R. M. (2013). *The international handbook of electronic commerce*. Routledge.
<https://doi.org/10.4324/9781315063218>
- 24) Sun, S., Law, R., & Schuckert, M. (2020). Mediating effects of attitude, subjective norms and perceived behavioural control for mobile payment-based hotel reservations. *International Journal of Hospitality Management*, 84, 102331.
- 25) Thi Tuyet Mai, N. (2019). An investigation into the relationship between materialism and green purchase behavior in Vietnam and Taiwan. *Journal of Economics and Development*, 21(2), 247-258.
- 26) Tasya, Aulia, Amanda., Endy, Gunanto, Marsasi. (2024). Image : *Jurnal Riset Manajemen*, 12(1):14-30.
doi: 10.17509/image.2024.002.
- 27) Victor, Andronatiev., Svetlana, Ceban. (2023). 6. Electronic Commerce. Competitiveness and Innovation in the knowledge economy, 1(1), 407-416.

The Impact of Consumer's Cyber-Fraud Perception on Purchase Behavior on E-Commerce through Perceived Behavioral Control

- 28) Wahab, F., Khan, I., Hussain, T., & Amir, A. (2023). An investigation of cyber attack impact on consumers' intention to purchase online. *Decision Analytics Journal*, 8, 100297.
- 29) Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal Justice*, 4(4), 451-489.
- 30) Rezk, A., Barakat, S., & Saleh, H. (2017). The impact of cyber crime on E-Commerce. *International Journal of Intelligent Computing and Information Sciences*, 17(3), 85-96. <https://doi.org/10.21608/IJICIS.2017.30055>
- 31) Shufiana, A., Sulhaini, S., & Saufi, A. (2021). The influence of attitude (ATTD), subjective norm (SN), perceived behavioral control (PBC), and self-efficacy (SE) on purchase intentions (INT) and behavior (BHV) using e-commerce. *International Journal of Multicultural and Multireligious Understanding*, 8(12), 123.
- 32) Yadav, R., & Pathak, G. S. (2017). Determinants of consumers' green purchase behavior in a developing nation: Applying and extending the theory of planned behavior. *Ecological economics*, 134, 114-122. <https://doi.org/10.1016/j.ecolecon.2016.12.019>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0)

(<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.