International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2027, 17(1), 289-298.

Cybercrime Awareness and Digital Purchasing Behavior among Generation Z Consumers: The Mediating Role of Perceived Cybersecurity Risk and Trust

Laurence P. Bazan[1], Mark Doblas[2]*, Randolf Von Salindo[2], Hearty Joy Chan[1], Lyndon Rosas[1], Diel Anthony R. Sagang[1], Marvin Tejol[1]

[1]Faculty, North Eastern Mindanao State University - Cantilan Campus, Cantilan Surigao del Sur, Philippines, [2]Faculty, Oman College of Management and Technology, Oman. *Email: mdoblas@ocmt.edu.om

Received: 15 May 2026 **Accepted:** 07 September 2026 **DOI:** https://doi.org/10.32479/irmm.24425

ABSTRACT

Cybercrime has become an increasing trend that causes fear about the safety of internet transactions, especially for Generation Z consumers. The present study examined the effect of cybercrime awareness on online purchase behavior with the mediating role of perceived cybersecurity risk and trust in e-commerce among 479 randomly sampled generation Z consumers from Cantilan, Surigao del Sur, Philippines. The study used a quantitative research method with a cross-sectional research design and data analyzed using partial least squares structural equation modeling (PLS-SEM). The study found that cybercrime awareness negatively affected perceived cybersecurity risk ($\beta = -0.627$, $P < 0.001$) and positively affected trust in e-commerce ($\beta = 0.602$, $P < 0.001$). On the other hand, the perception of cybersecurity risk had a negative impact on the digital purchase behavior ($\beta = -0.506$, $P < 0.001$), while the trust in e-commerce had a positive impact on the digital purchase behavior ($\beta = 0.443$, $P < 0.001$). Further, additional mediation analysis showed that both the perception of cybersecurity risk and the trust in e-commerce were significant mediators in the relationship between the awareness of cybercrime and the digital purchase behavior. This means that the awareness of cybercrime increases customer empowerment by increasing susceptibility and confidence in online transactions.

Keywords: Cybercrime Awareness, Digital Purchasing Behavior, Perceived Cybersecurity Risk, Trust in E-commerce, Generation Z
JEL Classifications: D83, D91, L81, M31, O33

1. INTRODUCTION

The development of digital technologies has changed the way of consumers to buy, making electronic commerce an integral part of the digital economy. The availability of online platforms for shopping has allowed consumers to gain more benefits, such as the convenience of purchase and more purchasing options. One generation that demonstrates its activity in the field of digital consumption is Generation Z. Digital technologies have been widely used by Generation Z for communication, monetary operations, and online shopping, which makes them one of the most active consumers in the digital economy (Pinter et al., 2021; Theocharis et al., 2025; Handoyo, 2024).

With the increasing number of e-commerce users, the risks of cybercrimes such as phishing scams, identity theft, financial scams, and data breaches are high (Mulla et al., 2026). In this context, there is growing concern about security and privacy in online transactions, which affects consumers' decision-making process and online shopping behavior (Tran and Nguyen, 2022; Phamthi et al., 2024). With increasing cyber threats in terms of both frequency and sophistication, there have been efforts made

This Journal is licensed under a Creative Commons Attribution 4.0 International License

to understand the determinants of consumer reactions towards such threats.

In relation to the elements that affect online consumer behavior, awareness about cybercrime has been increasingly researched by scholars. The individuals who have more information about cyber threats and cybersecurity are typically able to understand frauds, behave safely online, and make appropriate purchases (Herath et al., 2022; Pitchan et al., 2025). Nevertheless, the effect of cybercrime awareness on the perceptions of consumers in relation to cybersecurity risks is not unambiguously defined from the theoretical perspective. On the one hand, researchers argue that the higher level of awareness makes people perceive more cybersecurity risks due to the awareness of online dangers (Carvache-Franco et al., 2022; Lu, 2024). On the other hand, other studies emphasize that people who have higher levels of awareness feel less vulnerable online because they know more about cybersecurity, they are ready for possible problems, and are confident in online situations (Karwatzki et al., 2022; Shao et al., 2026).

Trust in the process of e-commerce can be yet another key factor which can make cybercrime awareness affect digital purchasing behavior. Given that there is uncertainty in the process of online transactions, people often use the concept of trust when making a decision about their engagement in digital transactions (Alzaidi and Agag, 2022; Singh et al., 2024). Research shows that the concept of trust promotes online purchases (Wang et al., 2022; Martínez-Navalón et al., 2023) while the perception of cybersecurity risks is likely to prevent people from engaging in such transactions (Soleimani, 2021; Faqih, 2022). Still, these concepts have not been studied together.

The extant literature also indicates that there are significant context-related research gaps. Most of the extant literature has been produced from advanced technological nations whereas empirical evidence based on local Filipino populations is quite sparse. Moreover, there is a lack of literature that is particularly focused on Generation Z consumers even though these consumers are increasingly becoming a part of the digital economy. There are certain unique patterns of technology usage among these consumers (Pinter et al., 2021; Theocharis et al., 2025).

In order to fill these research gaps, this research will explore the effects of cybercrime awareness on the purchase behavior of generation Z in relation to their digital purchases in Cantilan, Surigao del Sur, Philippines. In particular, this research will focus on how cybercrime awareness is affecting the digital purchase behavior of individuals due to the existence of cybersecurity risk and trust in e-commerce. Through the integration of these variables in one model, this research hopes to contribute to the existing literature on consumer behavior, cybersecurity, and e-commerce on the basis that it will help in understanding how cybercrime awareness affects the purchase behavior of individuals.

2. LITERATURE REVIEW

2.1. Cybercrime Awareness

With the continued growth of e-commerce, the consumers have been faced with more cybercrimes, hence cybercrime awareness becomes an important consideration for online purchase behavior. Cybercrime awareness is described as the knowledge and awareness of consumers about the dangers associated with cybercrimes and how one needs to be prepared against cybercrimes (Herath et al., 2022; Aslan et al., 2023). Awareness of cybercrime can help people to identify any scam activities and to behave responsibly in cyber space (Pitchan et al., 2025).

In case of Generation Z consumers, cybercrime awareness becomes especially relevant due to the wide usage of technologies for communication, money transfers, and buying goods online (Pinter et al., 2021; Theocharis et al., 2025; Handoyo, 2024). While members of Generation Z are highly active when using digital technologies, this makes them more vulnerable to different cybersecurity issues (Krishnaraj and Parveen, 2024). Therefore, the role of cybercrime awareness in consumer behavior has become an interesting topic that needs to be examined (Alzubaidi, 2021).

Cybercrime awareness has been shown to be a crucial factor determining the behavior of consumers while using the Internet in previous research works. Nonetheless, there is a discrepancy between different perspectives on the impact of cybercrime awareness on consumers' perception of online security. As illustrated by the research by Carvache-Franco et al. (2022) and Lu (2024) an increase in consumer awareness is associated with increased risks, whereas the findings by Karwatzki et al. (2022) and Shao et al. (2026) imply that increased awareness leads to increased knowledge and preparation for dealing with cyber-attacks.

2.2. Cybercrime Awareness and Perceived Cybersecurity Risk

The perceived cybersecurity risk is the personal assessment of the losses or threats that can happen when conducting electronic transactions (Phamthi et al., 2024). The threats include fraud, theft of personal identification data, breach of confidentiality, and unauthorized access to individuals' data, among others (Tran and Nguyen, 2022).

The literature presents two opposing views on the impact of cybercrime awareness on consumer-perceived cyber security risks. According to one view, increased awareness about cyber-crimes makes consumers feel higher levels of risk related to their cyber security, because people have more knowledge about the nature and impact of these crimes.

In contrast, according to Karwatzki et al. (2022), cybercrime awareness increases knowledge related to cybersecurity practices, allowing consumers to detect any threat and adopt necessary measures. With increased knowledge on the part of the consumers regarding safe practices of using the internet, it is possible that they

will feel more confident in their actions and thus less vulnerable even though they know about cyber threats (Shao et al., 2026). In this regard, one may state that awareness serves as a tool of empowerment for the consumers.

In view of the opposing theories mentioned above, there is a need for further empirical research on the effect of cybercrime awareness on cybersecurity risks among Generation Z. Therefore, the following hypothesis may be formulated:

- H_1. Cybercrime awareness significantly influences perceived cybersecurity risk.

2.3. Cybercrime Awareness and Trust in E-Commerce

Trust in e-commerce refers to the confidence of consumers in the security of online vendors and digital platforms in the transaction, protection of their personal information, and fulfillment of their obligation in online interactions (Singh et al., 2024). Given that the online transaction involves uncertainty and information asymmetry, trust is an important factor to reduce consumers' worries and encourage them in online commerce (Alzaidi and Agag, 2022; Doblas et al., 2025).

Cybersecurity awareness has been known as one of the significant antecedents of trust in online context (Lestari et al., 2024; Handoyo, 2024). Based on Tempestini et al., 2023, customers who have more knowledge about cybercrimes and cybersecurity are able to recognize a secure website, judge credibility of the online sellers, and discover frauds. Awareness of cybercrimes helps consumers to reduce uncertainty of online transactions and make a rational decision (Singh et al., 2024). In such a way, cybercrime awareness can help increase trust in e-commerce by helping consumers to differentiate fraudulent websites from legitimate ones (Maseeh et al., 2021).

Though many technological and organizational factors influence trust, consumer knowledge still remains a core process to develop confidence in online transactions (Chawla and Kumar, 2021). Consumers who know online security measures and safe online shopping practices are able to see reliability and safety of e-commerce sites and become willing to use them for their transactions (Wang et al., 2022). Hence, the following hypothesis can be stated:

- H_2. Cybercrime awareness significantly influences trust in e-commerce.

2.4. Perceived Cybersecurity Risk and Digital Purchasing Behavior

Perceived Cybersecurity risk is identified as an important factor that affects the consumer uptake of e-commerce (Soleimani, 2021; Serojai et al., 2021). Considering that the electronic transactions entail the transmission of personal and financial data, the possibility of experiencing identity theft, fraud, invasion of privacy, or hacking becomes an important aspect when making decisions (Handoyo, 2024). Due to high levels of cybersecurity risk perceptions, consumers become unsure about their decisions and do not want to conduct e-transactions (Faqih, 2022).

From the viewpoint of consumer behavior, people try to avoid risky decisions whenever they can. When talking about the risks of online shopping, concerns regarding transaction security or safety of personal information can cause consumers to avoid purchases on the internet or use other ways of purchasing products or services (Appiah and Agblewornu, 2025; Alrawad et al., 2023). Therefore, consumers who have higher perceptions of cybersecurity risk are unlikely to make e-purchases.

Although technological advances have led to constant improvement in online security technologies, cybersecurity risk remains an important factor affecting online purchases by consumers. Given this particular focus of Generation Z consumers who frequently shop online, it is crucial to understand the nature of the relationship in question. For this reason, the following hypothesis is put forward:

- H_3. Perceived cybersecurity risk significantly influences digital purchasing behavior.

2.5. Trust in E-Commerce and Digital Purchasing Behavior

Trust is one of the most important factors influencing consumer behavior on the Internet (Wang et al., 2022). Electronic commerce, as opposed to physical environments where shopping takes place, has features that do not involve any interaction between participants and a higher level of uncertainty about the quality of the goods and services provided, their safety, and the security of consumers' personal data (Qalati et al., 2021; Singh et al., 2024). Accordingly, trust plays a fundamental role in the decision of consumers to engage in online shopping. Sun and Qu (2025) have noted that the higher the trust in e-commerce platforms, the greater the consumers' perceptions of the security of online transactions, the protection of their privacy, and the fulfillment of obligations by the sellers. The lower the uncertainty involved in online shopping, the greater the readiness to complete the transactions in a digital environment (Martínez-Navalón et al., 2023). On the other hand, distrustful customers may avoid buying products online due to fears of security issues in spite of the convenient access to online services (Soleimani, 2021).

Since Generation Z has been relying on digital purchases more and more, the issue of trust should remain important while making a decision about purchasing something. Thus, consumer trust should be increased to encourage people to use e-commerce. Therefore, the following hypothesis can be formulated:

- H_4. Trust in e-commerce significantly influences digital purchasing behavior.

2.6. The Mediating Role of Perceived Cybersecurity Risk

The effect of cybercrime awareness on online purchase behavior may operate not only directly but also indirectly due to the perception of the consumer about cybersecurity risk. When consumers get informed about the cyber threats and measures for cybersecurity, their perception of the risk involved in the process of online purchase may shift (Kimpe et al., 2021; Krawczyk-Sokołowska and Caputa, 2023). Such an alteration affects their predisposition to conduct online purchases.

Perception of cybersecurity risk serves as a rational mediating construct that allows explaining the link between cybercrime awareness and online purchase behavior. Consumers whose perception of cybersecurity risks is low are more likely to use online purchases (Alrawad et al., 2023), while the high perception of such risks may negatively affect consumers' online purchases (Soares et al., 2022). Hence, the effect of cybercrime awareness on online purchase behavior may be explained by the perception of consumers about their vulnerability during online purchases.

Despite many separate investigations of the connections between cybercrime awareness, perceived risks, and online purchase behavior, little attention has been paid to the mediating role of the perception of cybersecurity risks, especially in the case of Generation Z consumers. The study of the above-mentioned relationship provides insight into how the cybersecurity awareness affects consumers. In this connection, the following hypothesis can be put forward:

- H_5. Perceived cybersecurity risk significantly mediates the relationship between cybercrime awareness and digital purchasing behavior.

2.7. The Mediating Role of Trust in E-Commerce

The second important mechanism by which the awareness of cybercrime can affect the digital purchase behavior is the trust in e-commerce (Becaro-Lapiz et al., 2026). With an increasing level of knowledge of the consumers regarding cyber threats and e-commerce security techniques, it becomes easier for people to assess the credibility of online vendors and the security measures that the e-commerce platforms take (Lu, 2024). The gained knowledge would increase the consumers' level of trust in online transactions and thus lead to digital purchasing behavior (Singh et al., 2024; Maseeh et al., 2021). Trust plays an essential intermediary role because it decreases the uncertainty of online transactions (Alzaidi and Agag, 2022). Consumers, who trust the e-commerce platform, are more likely to trust that their personal data would be safe, that the payment process is reliable, and the sellers would comply with their end of the bargain (Sun and Qu, 2025). Therefore, cybercrime awareness would encourage online purchasing through promoting increased confidence in the safety of digital marketplace (Wang et al., 2022).

While many researchers have proven the role of trust as one of the key factors of online consumer behavior (Martínez-Navalón et al., 2023), little attention has been paid to the mediating effect of trust in the cybercrime awareness – digital purchase behavior relationship, especially among Generation Z consumers. Investigating the mediating role of trust contributes to the understanding of the way in which knowledge of cybersecurity leads to active involvement in e-commerce activities (Tempestini et al., 2023). Thus, the following hypothesis can be formulated:

- H_6. Trust in e-commerce significantly mediates the relationship between cybercrime awareness and digital purchasing behavior.

2.8. The Research Gap

Although there is a growing body of research on cybersecurity and online consumer behavior, some limitations exist. To date, research has identified the importance of factors such as cybercrime awareness (Herath et al., 2022; Pitchan et al., 2025), cybersecurity risk perception (Soleimani, 2021; Faqih, 2022), and trust in e-commerce (Wang et al., 2022; Singh et al., 2024) for consumers' decision-making in relation to making purchases via the Internet. Still, each of the above-mentioned concepts has been analyzed separately, leaving a question unanswered about the psychological process of influence of cybercrime awareness on online shopping.

Furthermore, the existing research offers two alternative views on the relationship between cybercrime awareness and cybersecurity risk perception. According to one line of reasoning, increased awareness leads to a higher level of risk perception due to the fact that people gain better understanding of cyber threats (Carvache-Franco et al., 2022; Lu, 2024). Meanwhile, according to another view, increased awareness results in a higher level of security knowledge among consumers as well as their readiness to protect themselves from risks in online environment (Karwatzki et al., 2022; Shao et al., 2026).

Another important gap involves the lack of knowledge about the role played by perceived cybersecurity risk and trust in e-commerce together in the explanation of the impact of cybercrime awareness on digital purchasing behavior. Although earlier research has shown that each of these variables has its effect on online behavior independently (Alrawad et al., 2023; Martínez-Navalón et al., 2023; Soares et al., 2022; Wang et al., 2022), there is a lack of consideration about the complementary mediating role of these variables in explaining online consumer behavior. In addition, there is little empirical evidence regarding Generation Z consumers in local Philippine contexts although their involvement in the digital economy has increased.

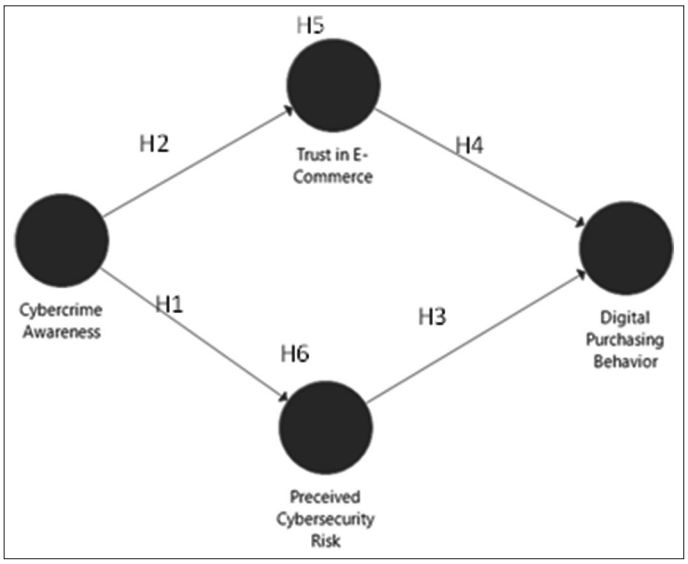
In this connection, the current study intends to conduct an analysis of the impact of cybercrime awareness on digital purchasing behavior of 479 Generation Z consumers from Cantilan, Surigao del Sur, Philippines using a framework that takes into account perceived cybersecurity risk and trust in e-commerce as mediators.

2.9. Conceptual Framework

Building on the review of relevant literature and gaps in existing knowledge, this study will develop an integrated theoretical framework describing how cybercrime awareness influences digital purchasing behavior among Generation Z consumers. According to the proposed framework in Figure 1, cybercrime awareness has a mediating impact on digital purchasing behavior via two psychological constructs – perceived cybersecurity risk and trust in e-commerce. Namely, cybercrime awareness is expected to affect perceived cybersecurity risk and trust in e-commerce, which then, in turn, are going to have an effect on digital purchasing behavior of the consumer.

Thus, the theoretical framework, as can be seen in Figure 1, constitutes the foundation for testing the research hypotheses developed in this study. Building on the proposed theoretical framework, six research hypotheses have been developed to explore the direct relationships between cybercrime awareness, perceived cybersecurity risk, trust in e-commerce and digital purchasing behavior, as well as mediating effects of perceived

Figure 1: Conceptual framework of the study



cybersecurity risk and trust in e-commerce on the latter one. They are outlined in sections 2.2 to 2.7.

3. METHODOLOGY

3.1. Research Design and Participants

The study employed quantitative and cross-sectional research methodology to determine the interrelationship of cybercrime awareness, cybersecurity risk perception, trust in e-commerce, and digital buying behavior of Generation Z customers. The study was conducted in Cantilan, Surigao del Sur, Philippines that involved 479 Generation Z customers who were randomly sampled to respond to the questionnaire survey.

The sample size adequacy was assessed according to modern criteria for partial least squares structural equation modeling (PLS-SEM). Hair and Alamer (2022) pointed out the importance of having enough statistical power to prove significance of any relationship within the structural model suggested. Having 479 valid answers, the sample significantly surpassed the minimum number of respondents required for this kind of models, and thus provided enough statistical power for estimation of the measurement and structural models, as well as testing hypotheses.

3.2. Research Instrument

The data collection instrument used was a structured questionnaire derived from existing validated questionnaires. The questionnaire comprised four latent variables which are cybercrime awareness, perceived cybersecurity risk, trust in e-commerce, and digital purchasing behavior. Items for cybercrime awareness construct were adapted from the Human Aspects of Information Security Questionnaire (HAIS-Q) created by Parsons et al. (2014). The items for perceived cybersecurity risk construct were adopted from the perceived risk scale created by Featherman and Pavlou (2003). Meanwhile, trust in e-commerce construct was measured using the trust scale constructed by McKnight et al. (2002). Lastly, the digital purchasing behavior construct was measured using the items adapted from Pavlou (2003).

Small changes have been made on the items to suit Generation Z consumers who engage in online shopping in the Philippines without changing the underlying meaning of the measurement items. All measurement scales were based on a five-point Likert scale where respondents were asked to rate from 1 (strongly disagree) to 5 (strongly agree) for each statement.

Before administering the main survey, the questionnaire went through content validity testing conducted by experts and pilot testing to test its clarity, relevance, and reliability. Psychometric property of the instrument was then determined using Cronbach's alpha (α), Composite Reliability (CR), Average Variance Extracted (AVE), and Heterotrait-Monotrait (HTMT) ratio.

3.3. Data Collection Procedure

Data gathering was conducted following the necessary permissions from the concerned authorities. Potential respondents were made aware of the purpose of the study, and their participation was completely voluntary. Their consent was taken before the conduct of the survey. The gathered data were validated and checked for consistency before encoding for analysis.

3.4. Data Analysis

Data analysis was conducted through SmartPLS 4, adopting the two-step analysis approach as recommended by Hair and Alamer (2022). The measurement model was assessed by evaluating the indicator loadings, variance inflation factors (VIF), Cronbach's alpha (α), composite reliability (CR), average variance extracted (AVE), and HTMT ratio for indicator reliability, internal consistency reliability, convergent validity, discriminant validity, and collinearity, respectively.

Subsequently, the structural model was analyzed with the use of bootstrapping procedure involving 5,000 resamples to test the significance of the hypothesized direct and indirect relationships. Path coefficients (β), standard errors, t-values, and P-values were employed in evaluating the hypotheses. Furthermore, the mediating role of perceived cybersecurity risk and trust in e-commerce was also investigated through specific indirect effects using the bootstrapping technique.

Since the data on all study constructs were obtained from the same subjects using one instrument, procedural controls were adopted to control the effect of common method variance. This involved the assurances regarding the confidentiality and anonymity of responses, voluntary participation and the use of questionnaire items drawn from previously tested scales.

3.5. Ethical Considerations

The study respected the existing ethical guidelines that guide any research involving human subjects. All participants in the research process volunteered in giving their consent after learning about the aim of the research. The research remained anonymous, confidential, and no personal data was collected in the entire process. The data collected in the research process was for academic purposes only and the respondents knew that they had the right to quit the study at any point without any penalties.

Table 1: Internal consistency and convergent validity

Construct	Factor	VIF	Loading	AVE	α	CR
Cybercrime Awareness (CyA)	CyA1	4.892	0.931	0.848	0.955	0.965
	CyA2	4.376	0.915			
	CyA3	4.599	0.910			
	CyA4	5.345	0.933			
	CyA5	4.259	0.917			
Perceived Cybersecurity Risk (PCR)	PCR1	3.962	0.910	0.777	0.928	0.946
	PCR2	2.400	0.835			
	PCR3	3.583	0.901			
	PCR4	3.409	0.895			
	PCR5	2.875	0.865			
Trust in E-Commerce (Trust)	Trust1	2.547	0.860	0.778	0.928	0.946
	Trust2	2.531	0.865			
	Trust3	5.470	0.905			
	Trust4	6.255	0.923			
	Trust5	2.652	0.855			
Digital Purchasing Behavior (DPB)	DPB1	4.370	0.923	0.817	0.944	0.957
	DPB2	3.679	0.910			
	DPB3	4.035	0.908			
	DPB4	4.897	0.928			
	DPB5	2.514	0.849			

4. RESULTS AND DISCUSSION

4.1. Profile of the Respondents

There were 479 valid questionnaires that were used in the analysis. Information about demographics of the respondents was given based on their age and gender. In relation to age, most of the respondents were 18-20 years of age, representing 41.34% (n = 198) of the sample. Respondents who were older than 20 years made up 39.67% (n = 190) of the sample, while those younger than 18 years accounted for 18.99% (n = 91) of the respondents. In regard to gender, female respondents formed 58.46% (n = 280) of the sample.

4.2. Construct Validity

The reliability and convergent validity of the measurement model have been analyzed using the following criteria – factor loadings, variance inflation factor (VIF), Cronbach's alpha (α), composite reliability (CR) and average variance extracted (AVE). All the factor loadings, as shown in Table 1 below, are above the desired level of 0.70, which lies between 0.835 and 0.933, thus demonstrating that the observed indicators have appropriately measured their corresponding latent variables. In addition, the variance inflation factors range from 2.400 to 6.255.

Furthermore, there was good evidence of internal consistency reliability in the constructs. The Cronbach's alpha scores were between 0.928 and 0.955, whereas the composite reliability scores were between 0.946 and 0.965, which exceed the minimum standard of 0.70. This means that there is a high degree of consistency between the indicators that measure each construct. Additionally, the AVE scores were between 0.777 and 0.848, which all exceeded the threshold score of 0.50, thereby indicating good convergent validity. Taken together, this suggests good indicator reliability, internal consistency and convergent validity of the measurement model.

Table 2 provides the results for heterotrait-monotrait (HTMT) ratio that is used to evaluate discriminant validity between

Table 2: Discriminant validity Heterotrait–Monotrait (HTMT) ratio

Construct	CyA	PCR	Trust	DPB
Cybercrime Awareness (CyA)				
Perceived Cybersecurity Risk (PCR)	0.662			
Trust in E-Commerce (Trust)	0.640	0.709		
Digital Purchasing Behavior (DPB)	0.615	0.852	0.826	

study constructs. The values of HTMT range from 0.615 to 0.852. All these values are less than the conservative value of 0.90, thus signifying that the constructs under consideration are empirical distinguishable from each other and have satisfactory discriminant validity. Even though the value of HTMT between Perceived Cybersecurity Risk and Digital Purchasing Behavior (HTMT = 0.852) is the highest among all the pairs of constructs, it is still lower than the recommended critical value, which indicates satisfactory discriminant validity (Hair and Alamer, 2022).

4.3. Path Analysis

The results of the structural model analysis are presented in Table 3. As a result of the analysis, it was found that cybercrime awareness had a statistically significant negative impact on the perception of cybersecurity risks ($\beta = -0.627$, $t = 25.996$, $P < 0.001$). This means that the generation Z consumers with high levels of cybercrime awareness experience low perceptions of cybersecurity risks.

Furthermore, cybercrime awareness had a statistically significant positive impact on trust in e-commerce ($\beta = 0.602$, $t = 22.961$, $P < 0.001$). Therefore, it can be concluded that people who have high awareness of cybercrimes are more likely to trust online shopping websites.

Regarding the digital purchase behavior, perception of cybersecurity risk had a statistically significant negative impact ($\beta = -0.506$, $t = 10.081$, $P < 0.001$), while trust in e-commerce had a statistically significant positive impact ($\beta = 0.443$, $t = 9.252$, $P < 0.001$). It means that people who experience high levels of cybersecurity risks are not inclined to make purchases in the Internet, while those who trust the website of the online store make more purchases online.

The outcomes for the mediation analysis were found to be significant. Cybercrime awareness had a negative and significant influence on the digital purchase behavior via the variable of cybersecurity risk perception ($\beta = -0.317$, $t = 9.567$, $P < 0.001$), thus verifying Hypothesis 5. Moreover, cybercrime awareness had a significant influence on the digital purchase behavior via the variable of e-commerce trust ($\beta = 0.266$, $t = 9.306$, $P < 0.001$), thus verifying Hypothesis 6.

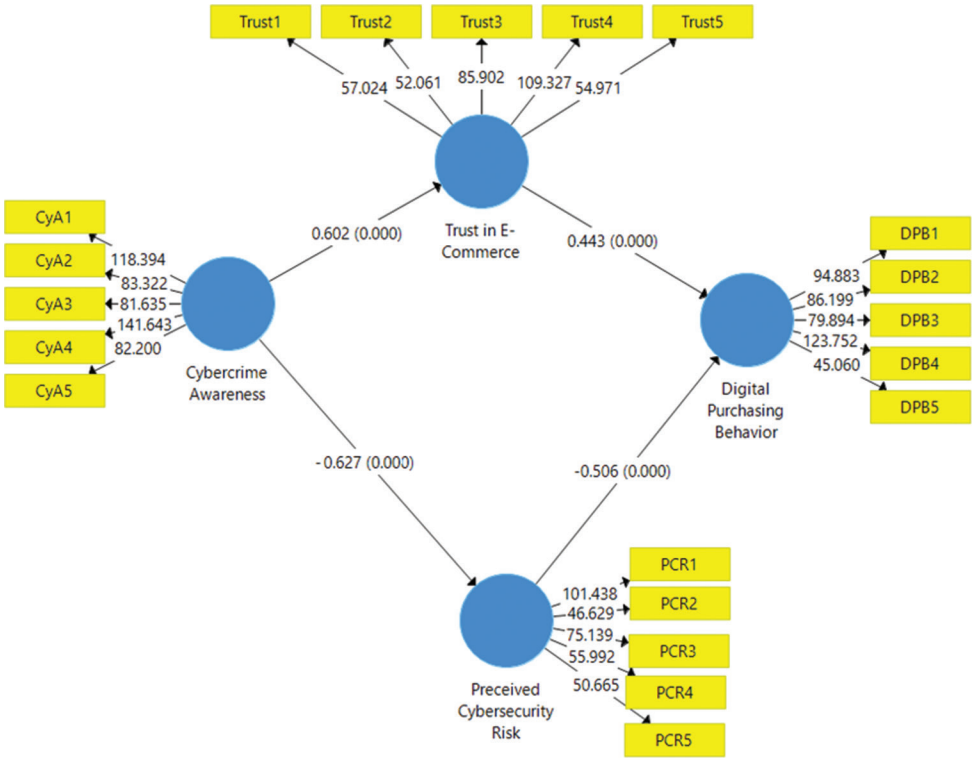
In sum, Figure 2 depicts the structural model along with the importance of the hypothesized relationships between the research variables. The findings show that all structural paths have statistical significance at $P < 0.001$. Particularly, cybercrime awareness is found to have a positive impact on the trust in e-commerce ($\beta = 0.602$), but it is negatively related to the level of cybersecurity

Table 3: Summary of hypothesis testing results for direct and indirect effects

Path	H	β	SD	t	P	Decision
Direct Effects						
Cybercrime Awareness→Perceived Cybersecurity Risk	H_1	−0.627	0.024	25.996	<0.001	Accepted
Cybercrime Awareness→Trust in E-Commerce	H_2	0.602	0.026	22.961	<0.001	Accepted
Perceived Cybersecurity Risk→Digital Purchasing Behavior	H_3	−0.506	0.050	10.081	<0.001	Accepted
Trust in E-Commerce→Digital Purchasing Behavior	H_4	0.443	0.048	9.252	<0.001	Accepted
Indirect Effects (Mediation via Perceived Cybersecurity Risk)						
Cybercrime Awareness→Perceived Cybersecurity Risk→Digital Purchasing Behavior	H_5	−0.317	0.033	9.567	<0.001	Accepted
Indirect Effects (Mediation via Trust in E-Commerce)						
Cybercrime Awareness→Trust in E-Commerce→Digital Purchasing Behavior	H_6	0.266	0.029	9.306	<0.001	Accepted

β=Standardized path coefficient, SD=Standard deviation. Significance was assessed using bootstrapping with 5,000 resamples. Paths with P<0.05 were considered statistically significant

Figure 2: Structure model assessment



risks (β = −0.627). Furthermore, the trust in e-commerce is significantly positively related to the digital purchasing behavior (β = 0.443), while cybersecurity risk is negatively associated with digital purchasing behavior (β = −0.506). The bootstrapping t-value for the measurement items and structural paths is higher than the suggested value.

4.4. Theoretical Implications

This study considered the associations between cybercrime awareness, cybersecurity risk perception, e-commerce trust, and the digital purchase behavior of Gen Z consumers. Generally, the empirical evidence gathered from this study strongly supported the proposed model as all hypotheses tested in the model proved to be true and statistically significant. This study has revealed that cybercrime awareness impacts digital purchase behavior through two interrelated psychological processes – cybersecurity risk reduction and e-commerce trust.

Perhaps, one of the most interesting findings of this study is the negative association between cybercrime awareness and cybersecurity risk perception. The results do not conform to the common assumption that people with more cyber threat awareness consider themselves to be more susceptible to cyber security threats (Carvache-Franco et al., 2022; Lu, 2024). Nevertheless, these finding gains theoretical meaning when cybercrime awareness is not considered merely as awareness of the presence of certain dangers but as some kind of knowledge and competence. Indeed, having high levels of cybercrime knowledge, a person would be better able to distinguish between fraudulent behavior, find reliable sources on the Internet, and implement security measures. In such a way, despite being aware of the dangers of cybercrimes, people feel less exposed to these risks during online purchases.

Furthermore, the study also showed that cybercrime awareness played an important role in promoting trust in e-commerce. It can be inferred that rather than being a factor that prevents people from using technology, awareness helps people to use technology in a much wiser manner. With the help of cybercrime awareness, consumers have more ability to identify the authenticity of online vendors. In addition, cybersecurity knowledge is also an important

determinant of trust in digital environment (Lestari et al., 2024; Tempestini et al., 2023).

Perceived cybersecurity risk had a significant negative effect on digital purchasing behavior. Consumers having higher level of cybersecurity risk perception are less inclined to indulge in online shopping due to the fear of losing money, identity fraud, privacy violations, and any fraudulent transaction. This finding is consistent with other empirical studies in which cybersecurity risk is found to be a crucial barrier to e-commerce adoption (Faqih, 2022; Alrawad et al., 2023).

In contrast, the relationship between e-commerce trust and digital purchasing behavior was found to be positive, thus validating the assertion that trust is one of the strongest predictors of individuals' willingness to transact on-line. Individuals with trust in e-commerce regarding security, protection of personal data, and ethics of transaction are more prone to engage in online transactions. This result further validates the findings of earlier researches stressing the significance of trust as a key facilitating factor for engaging in e-commerce and online transactions (Wang et al., 2022; Martínez-Navalón et al., 2023).

Moreover, the mediation analysis helps to shed more light on the ways in which cybercrime awareness impacts digital purchasing behavior. The presence of statistically significant indirect effects suggests that cybercrime awareness affects individuals' behavior through two mediators, which are reducing the perception of cybersecurity risk and trust in e-commerce.

In terms of theory, this research adds to the body of literature on cybersecurity and e-commerce through the conceptual distinction between cybercrime awareness and the perception of cybersecurity risk. Despite their presumed tendency to rise together, the current results indicate that the higher the level of cybercrime awareness is, the lower the perception of cybersecurity risk becomes, assuming that this awareness stands for consumers' understanding of cyber threats and readiness to deal with them. The proposed distinction contributes to current theories about consumer online behavior, proving that education in cybersecurity does not necessarily raise consumer concern.

The results can also provide some useful applications for policymakers, schools, and e-commerce companies. Not only should the awareness campaigns be geared towards making the consumers aware of the cyber risks, but also, they should aim at building digital security skills that help boost consumers' confidence in their online protection. Similarly, the e-commerce companies should keep on implementing measures like the presence of security tools, clear privacy policies, safe payments, and consumer education campaigns in order to minimize the cyber risk.

5. CONCLUSION

This research contributes to the existing literature on consumer behavior in the digital space by providing empirical evidence that cybercrime awareness plays a role in shaping Generation Z consumers' online buying decisions by means of complementary factors of perceived cybersecurity risk and trust in e-commerce. In particular, it was found that consumers' reactions to the risks arising from the digital market environment depend not only on the way consumers perceive these risks but also on consumers' ability to cope with risks and trust in e-commerce.

One important contribution of this research is its demonstration of the negative correlation between cybercrime awareness and perceived cybersecurity risk. This finding implies that consumers should be encouraged to acquire cybercrime awareness as a factor which empowers consumers with knowledge and confidence in coping with risks rather than makes consumers more scared about cyber risks.

Moreover, the study emphasizes the critical role of trust as a core driver of digital purchasing decisions. On the whole, findings imply that programs designed for the promotion of safe online transactions should go beyond increasing people's awareness about potential dangers of the cyberspace to include the development of digital skills of consumers and increase their trust in the safety of online transactions.

However, despite its numerous strengths, there are a number of limitations that the research suffers from. First of all, cross-sectional design prevents establishing cause-and-effect relationships between dependent and independent variables. Furthermore, the fact that the sample is limited only to Generation Z consumers may reduce the ability to generalize the results obtained for other age groups and types of consumers. In the future, other studies may adopt longitudinal and experimental designs in order to prove the cause-and-effect relationships identified in the current paper and investigate whether they are valid for different demographic, cultural and e-commerce contexts. It is also possible to conduct other studies with a combination of other psychological and technological factors, such as cybersecurity self-efficacy, privacy, digital literacy and institutional trust.

In conclusion, this study makes an addition to the existing literature on cybersecurity and e-commerce, since it shows that being informed about security issues does not necessarily mean being afraid of them. On the contrary, cybercrime awareness leads to informed decision making and increases trust of the consumers.

REFERENCES

Alrawad, M., Lutfi, A., Alyatama, S., Khattab, A.A., Alsoboa, S.S., Almaiah, M.A., Ramadan, M., Arafa, H.M., Ahmed, N., Alsyouf, A., Al-Khasawneh, A. (2023), Assessing customers perception of online shopping risks: A structural equation modeling-based multigroup analysis. Journal of Retailing and Consumer Services, 71, 103188.

Alzaidi, M., Agag, G. (2022), The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. Journal of Retailing and Consumer Services, 68, 103042.

Alzubaidi, A. (2021), Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7, e06016.

Appiah, T., Agblewornu, V.V. (2025), The interplay of perceived benefit, perceived risk, and trust in FinTech adoption: Insights from Sub-

Saharan Africa. Heliyon, 11, e41992.
Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yılmaz, A.A., Akin, E. (2023), A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
Becaro-Lapiz, J.M., Ronquillo, M.N.R., Dingding, R., Beliganio, A., Baynosa, G., Doblas, M. (2026), AI-generated influencers and purchase intention: The mediating role of trust and attitude in HEIs in Southern Philippines. International Review of Management and Marketing, 16(4), 787-796.
Carvache-Franco, O., Loaiza-Torres, J., Soto-Montenegro, C., Carvache-Franco, M., Carvache-Franco, W. (2022), The risks perceived by the consumer in the acceptance of electronic commerce. A study of Bolivia. PLoS One, 17, e0276853.
Chawla, N., Kumar, B. (2021), E-Commerce and consumer protection in India: The emerging trend. Journal of Business Ethics, 180, 581-604.
Doblas, M., Rajab, F., Salman, W., Alabbas, A., Salindo, R. (2025), Influence of digital commerce and mobile point-of-sale payments on bank risk and performance in Bahrain: A dynamic panel analysis. Risk Governance and Control Financial Markets and Institutions, 15(2), 134-147.
Faqih, K. (2022), Internet shopping in the Covid-19 era: Investigating the role of perceived risk, anxiety, gender, culture, and trust in the consumers' purchasing behavior from a developing country context. Technology in Society, 70, 101992.
Featherman, M.S., Pavlou, P.A. (2003), Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451-474.
Hair, J.F., Alamer, A. (2022), Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. Research Methods in Applied Linguistics, 1, 100027.
Handoyo, S. (2024), Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. Heliyon, 10, e29714.
Herath, T.B., Khanna, P., Ahmed, M. (2022), Cybersecurity practices for social media users: A systematic literature review. Journal of Cybersecurity and Privacy, 2, 1-18.
Karwatzki, S., Trenz, M., Veit, D.J. (2022), The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. Information Systems Journal, 32, 1126-1157.
Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K. (2021), What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour and Information Technology, 41, 1796-1808.
Krawczyk-Sokołowska, I., Caputa, W. (2023), Awareness of network security and customer value - the company and customer perspective. Technological Forecasting and Social Change, 190, 122430.
Krishnaraj, R., Parveen, S. (2024), Vulnerability of Gen-Z to E-commerce deception on consumer's belief categories in online product recommendations systems. Quality Innovation Prosperity, 28, 151.
Lestari, S., Adawiyah, W.R., Alhamidi, A.L., Prayogi, J., Haryanto, R. (2024), Navigating perilous seas: Unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4), 444-464.
Lu, F. (2024), Online shopping consumer perception analysis and future network security service technology using logistic regression model. PeerJ Computer Science, 10, e1777.
Martínez-Navalón, J.G., Fernández-Fernández, M., Alberto, F.P. (2023), Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? International Entrepreneurship and Management Journal, 19, 781-803.
Maseeh, H.I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., Ashaduzzaman, M. (2021), Privacy concerns in e-commerce: A multilevel meta-analysis. Psychology and Marketing, 38, 1779-1798.
McKnight, D.H., Choudhury, V., Kacmar, C. (2002), Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-359.
Mulla, G., Doblas, M., Bazan, L., Maganding, L.M. (2026), Cybercrime preparedness and the digital economy: Empirical evidence in MENA and South Asia using Driscoll-Kraay. In: Sustainable Innovations in Management in the Digital Transformation Era. United States: CRC Press. p380-385.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014), Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers and Security, 42, 165-176.
Pavlou, P.A. (2003), Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3), 101-134.
Phamthi, V.A., Nagy, Á., Ngo, T.M. (2024), The influence of perceived risk on purchase intention in e-commerce-systematic review and research Agenda. International Journal of Consumer Studies, 48(4), e13067.
Pinter, É., Bagó, P., Berényi, L., Molnár, L., Deutsch, N., Szigeti, G., Pintér, T. (2021), How do digitalization and the FinTech phenomenon affect financial decision-making in the younger generation? Acta Polytechnica Hungarica, 18(11), 191-208.
Pitchan, M.A., Salman, A., Arib, N.M. (2025), A systematic literature review on online scams: Insights into digital literacy, technological innovations, and victimology. Jurnal Komunikasi Malaysian Journal of Communication, 41(1), 107-124.
Qalati, S.A., Vela, E.G., Li, W., Dakhan, S., Thuy, T.T.H., Merani, S.H. (2021), Effects of perceived service quality, website quality, and reputation on purchase intention: The mediating and moderating roles of trust and perceived risk in online shopping. Cogent Business and Management, 8, 1869363.
Serojai, A.T.B., Ujir, H.B., Hipiny, I.H.B.M. (2021), E-Commerce Readiness assessment in Sarawak. Acta Informatica Pragensia, 10, 192-206.
Shao, S., Bie, X., Kim, J.M. (2026), From digitalization awareness to consumer outcomes: The sequential roles of risk appraisal and platform trust in the Chinese E-commerce context. Journal of Theoretical and Applied Electronic Commerce Research, 21, 168.
Singh, N., Misra, R., Quan, W., Radic, A., Lee, S.M., Han, H. (2024), An analysis of consumer's trusting beliefs towards the use of e-commerce platforms. Humanities and Social Sciences Communications, 11, 1-18.
Soares, J.C., Limongi, R., De Sousa Júnior, J.H., Santos, W.S., Raasch, M., Hoeckesfeld, L. (2022), Assessing the effects of COVID-19-related risk on online shopping behavior. Journal of Marketing Analytics, 11, 82-94.
Soleimani, M. (2021), Buyers' trust and mistrust in e-commerce platforms: A synthesizing literature review. Information Systems and e-Business Management, 20, 57-78.
Sun, Y., Qu, Q. (2025), Platform governance, institutional distance, and seller trust in cross-border E-Commerce. Behavioral Sciences, 15, 183.
Tempestini, G., Rovira, E., Pyke, A.A., Nocera, F.D. (2023), The cybersecurity awareness inventory (CAIN): Early phases of development of a tool for assessing cybersecurity knowledge based on the ISO/IEC 27032. Journal of Cybersecurity and Privacy, 3, 61-75.

Theocharis, D., Tsekouropoulos, G., Chatzigeorgiou, C., Kokkinis, G. (2025), Empirical categorization of factors affecting online consumer behavior of gen Z regarding newly launched technological products and moderating impact of perceived risk. Behavioral Sciences, 15, 371.

Tran, V., Nguyen, T.D. (2022), The impact of security, individuality, reputation, and consumer attitudes on purchase intention of online shopping: The evidence in Vietnam. Cogent Psychology, 9, 2035530.

Wang, J., Shahzad, F., Ahmad, Z., Abdullah, M., Hassan, N.M. (2022), Trust and consumers' purchase intention in a social commerce platform: A meta-analytic approach. SAGE Open, 12, 1-15.