Assessing the Relationship between Young Professionals' Perceptions of Cyber security and Their Online Shopping Behaviour on E-Commerce Platforms in Koronadal City, Philippines

Jayson Diaz
Green Valley College
jdiaz@gvcfi.edu.ph

Purpose This study investigates the relationship between young professionals' perceptions of cyber security and their level of online shopping on e-commerce platforms in Koronadal City.

Study design/methodology/approach: A descriptive-correlational research design was employed to assess the socio-economic profile, cyber security concerns, and personal risk mitigation practices of 68 young professionals. Data were collected using a structured survey instrument and analyzed through frequency distribution, weighted mean, standard deviation, and simple linear regression.

Findings: The majority of respondents were aged 27 to 30, earned below PHP 10,000 monthly, and were primarily self-employed. Participants expressed high concerns regarding the security of personal and financial information, with data security being the highest concern (mean = 4.57). A significant inverse relationship was found between cybersecurity concerns and the level of e-commerce usage (β = -0.179, p = 0.046), indicating that greater concerns about cybersecurity led to lower online shopping frequency. Personal risk mitigation practices were moderate, with respondents frequently updating passwords and exercising caution with suspicious links, though the use of two-factor authentication remained inconsistent.

Originality/value: This study provides empirical insights into how cybersecurity concerns influence online shopping behavior among young professionals. The findings emphasize the need for e-commerce platforms to enhance security measures and transparency to improve consumer confidence. Additionally, the study underscores the importance of targeted cybersecurity education to encourage safer and more frequent e-commerce engagement.

Introduction

In today’s digital age, cyber security in e-commerce platforms is a growing concern worldwide, especially as e-commerce has expanded rapidly across various demographics, including young professionals. Globally, cyber security risks in online transactions continue to increase, with cybercrime projected to reach $10.5 trillion annually by 2025 (Wallang et al., 2022). As more individuals engage in online shopping, securing sensitive data such as payment information, personal addresses, and identification numbers has become critical. According to a survey by Toleuuly et al. (2020), consumers’ trust in e-commerce platforms heavily depends on the perceived security of these websites, with young, digitally savvy users expressing heightened concerns about data breaches. Given the frequency of online transactions, young professionals worldwide are increasingly vigilant about cyber security, which directly affects their online shopping behaviors.

In the Philippines, the rise of e-commerce platforms has accelerated, especially during the COVID-19 pandemic. According to the Department of Trade and Industry (DTI, 2021), online shopping in the Philippines grew by 55% between 2020 and 2021, reflecting a shift towards e-commerce platforms. However, this shift has also brought heightened cyber security concerns, as reports of phishing and online fraud have surged alongside this growth (Philippine Statistics

Authority [PSA], 2022). Filipino young professionals, who constitute a large portion of the country's digital consumer base, are particularly susceptible to these risks given their high level of engagement with e-commerce platforms. With limited local studies focusing specifically on young professionals' cyber security perceptions, there is an increasing need for insights into how this demographic perceives the safety of their online shopping experiences.

Locally, in Koronadal City, online shopping has also gained traction among young professionals, yet limited studies have explored the specific cyber security concerns of this group. As e-commerce platforms such as Lazada, Shopee, and Shein grow in popularity, understanding the cyber security perceptions of young professionals in Koronadal is essential for local policymakers and businesses. Diaz et al. (2023) noted that despite the increase in online shopping among Koronadal's young professionals, awareness of cyber security measures remains uneven, with some individuals feeling confident in the platform's security measures and others expressing concerns about potential data breaches. This local context highlights the need for further research to address cyber security awareness and evaluate whether the current e-commerce platforms meet the security expectations of young professionals in Koronadal City.

While several studies have investigated cyber security in general online transactions, there is a lack of research specifically focusing on young professionals' perceptions of cyber security on e-commerce platforms in smaller cities like Koronadal. Most cyber security studies concentrate on national and metropolitan contexts, leaving a gap in understanding regional perspectives, especially in areas where online shopping is growing but not yet deeply ingrained. Addressing this gap could provide valuable insights into the concerns and trust factors that affect young professionals' engagement with e-commerce in Koronadal.

The main objective of this study is to assess young professionals' perceptions of cyber security on e-commerce platforms in Koronadal City. By identifying key factors influencing their trust and security concerns, this research aims to provide insights that could help local e-commerce providers enhance cyber security measures and align their strategies with the expectations of young, professional consumers.

Literature Review

Cyber security Concerns of Customers

Cyber security concerns are a significant factor influencing consumer confidence in online shopping. Data usage is a major issue, with many consumers worried about how their personal data is collected, stored, and shared by e-commerce platforms (Omar et al., 2020). Consent and transparency are also critical, as customers increasingly demand clear and honest communication regarding the use of their data, especially in terms of opt-ins for marketing and data-sharing practices. Additionally, security measures such as encryption, authentication, and fraud protection are key to gaining and maintaining consumer trust in e-commerce platforms (Chellappa & Pavlou, 2002).

Level of Usage in E-Commerce Platforms

The extent of online shopping usage is directly influenced by factors such as platform usability, trust, and product variety. Studies reveal that consumers are more likely to engage with e-commerce platforms that offer easy navigation, secure payment options, and a wide range of products (Davis et al., 2021). Furthermore, trust in the platform's security protocols has been shown to correlate with a higher frequency of online purchases, as users are more willing to share sensitive information when they feel their data is protected (Tarhini et al., 2018).

Personal Risk Mitigation Practices

Young professionals tend to employ various personal risk mitigation practices when shopping online, such as using strong passwords, regularly monitoring bank statements, and avoiding transactions on unsecured networks (Frimfong et al., 2021). Research has shown that consumers who engage in these practices are more likely to feel secure while making online purchases and report a higher level of satisfaction with e-commerce platforms (Kim & Vonortas, 2018). These practices are critical in reducing perceived risks and fostering a sense of security during online transactions.

Relationship between Cyber security Perceptions and Level of Usage

Several studies have indicated a significant linear relationship between cyber security perceptions and online shopping behaviour. As cyber security concerns decrease, consumers are more likely to engage with e-commerce platforms and make frequent purchases (Haddad et al., 2021). Conversely, a lack of trust in platform security can lead to decreased usage and a higher tendency to abandon shopping carts (Kedah 2023). This relationship underscores the importance of enhancing security measures to boost consumer confidence and encourage higher levels of engagement with e-commerce platforms.

Theoretical Framework

This study is primarily grounded in the Protection Motivation Theory (PMT), which is used to understand how individuals assess threats and the protective behaviours they adopt in response to those threats. Developed by Rogers (1975), PMT posits that individuals' decision to engage in protective behaviours is influenced by their perceptions of the severity and vulnerability of a threat, as well as the efficacy of their protective responses and their ability to execute those responses.

In the context of this study, PMT helps explain how young professionals' perceptions of cyber security risks on e-commerce platforms influence their behaviour regarding online shopping. Specifically, the theory suggests that if young professionals perceive cyber security threats (such as data breaches or fraud) as severe and personally relevant, they will be more likely to engage in protective behaviours, such as adopting secure payment methods, using strong passwords, or limiting personal information shared on e-commerce platforms. The extent to which individuals feel vulnerable to these threats also plays a role in their adoption of these protective actions.

Furthermore, PMT emphasizes the role of response efficacy (belief in the effectiveness of a protective behaviour) and self-efficacy (belief in one's ability to carry out the protective behaviour). In this study, young professionals' perceptions of the effectiveness of cyber security measures (such as encryption, secure payment gateways, or two-factor authentication) on e-commerce platforms, as well as their confidence in implementing these measures, are key factors in determining the level of their online shopping engagement. Thus, PMT provides a robust framework for exploring how young professionals' cyber security concerns influence their online shopping behaviour, guiding this study's investigation into the relationship between cyber security perceptions and online shopping usage on e-commerce platforms.

Conceptual Framework

This study explores the relationship between young professionals' cyber security perceptions and their online shopping behaviours on e-commerce platforms, based on Protection Motivation Theory (PMT). The key variables in the framework include perceptions of cyber security, which assess how young professionals perceive the severity and vulnerability of online threats like data breaches, and their evaluation of security measures on platforms. Online shopping behaviour refers to the frequency and extent to which individuals engage with e-commerce platforms, influenced by their perceptions of security risks. Finally, personal risk mitigation practices cover the actions young professionals take to protect themselves, such as using secure payment methods and managing passwords. This framework examines how perceptions of cyber security risks shape shopping behaviour, with personal risk mitigation acting as a key factor in online shopping engagement.

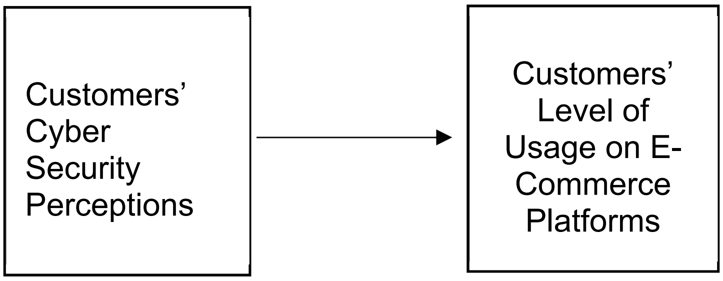
Customers' Cyber Security Perceptions
Customers' Level of Usage on E-Commerce Platforms

Figure 1. Conceptual Paradigm

Research Objectives

The main objective of this study is to explore the relationship between young professionals' perceptions of cyber security and their online shopping behavior on e-commerce platforms.

Specifically, this study aims to:

1. To Determine the socio-economic profile of the customers in terms of:
   1.1 Age
   1.2 Sex; and
   1.3 Monthly Income level
   1.4 Employment status
2. To determine the cybersecurity concerns of the customers in the e-commerce platforms:
   2.1 Data usage
   2.2 Consent and transparency
   2.3 Security measures
3. To determine the customers' level of usage in e-commerce platforms.
4. To determine the level of personal risk mitigation practices of the young professional customers.
5. To determine the significant linear relationship between the perception in cybersecurity concerns and level of usage on e-commerce platforms.

Scope and Limitations

This study focuses on assessing young professionals' perceptions of cyber security and its relationship with their online shopping behavior on e-commerce platforms in Koronadal City. It examines variables such as demographic characteristics, cyber security concerns (data usage, consent, security measures), and personal risk mitigation practices. However, the study is limited in its scope, as it focuses solely on young professionals aged 18-35 who are currently employed, meaning the findings may not be representative of other age groups or unemployed individuals. Potential biases, such as self-reporting and social desirability bias, may also affect the accuracy of respondents' answers. Furthermore, the study's results may not be easily generalized to other regions or consumer segments, as it is specific to Koronadal City and platforms like Shopee, Shein, and Lazada. The application of the findings is mainly relevant to e-commerce businesses and policymakers in the local context, and while the research provides valuable insights, the evolving nature of e-commerce and cyber security may require further studies to validate these results over time.

Research Methodology

Research Design

This study adopted a descriptive correlational design to examine the relationship between young professionals' perceptions of cyber security and their online shopping behaviors on e-commerce platforms. This design was appropriate as it allowed for the exploration of existing patterns between cyber security perceptions, shopping behavior, and personal risk mitigation without manipulating variables. The descriptive component enabled the study to gather detailed information on respondents' perceptions of security and shopping habits, while the correlational aspect examined the strength and direction of the relationship between these variables. This approach provided valuable insights into how cyber security concerns influenced online shopping behavior.

Sampling Technique

This study utilized a convenience sampling technique to select respondents who were young professionals in Koronadal City, aged 18 to 35, employed, and actively engaging in online shopping. However, due to the lack of specific data on the total population of young professionals in Koronadal City, the researcher was unable to determine an exact population size for the sample. To address this, the researcher used Cochran's formula to calculate the appropriate sample size. Cochran's formula is commonly used in research to estimate a sample size when the population is unknown or unspecified. This method helped ensure that the sample size was sufficiently large to yield reliable results while maintaining statistical validity. While the convenience sampling method allowed for easy access to participants, it also meant that the sample may not fully represent the broader population of young professionals in Koronadal City.

Sample size calculation

Sample for unknown population using (Cochran, 1977) Formula.
$n = z^{2\,(}\sigma \text{ x } (1- \sigma))/E^2$
$Z = z$ -Score (90%= 1.645)
σ + standard deviation at 0.5
E = Margin of Error (E = 0.10)
$N = 1.645^2 \quad \text{x } 0.5) / 0.1^2$
n = 68 respondents

Respondents

The respondents for this study were young professionals in Koronadal City, aged 18 to 35, who were employed full-time or part-time and actively engaged in online shopping through platforms like Shopee, Lazada, and Shein. This age group was selected due to their frequent use of e-commerce platforms and awareness of cyber security issues. The study utilized convenience sampling, where participants were selected based on their availability and willingness to participate.

Research Instrument

The research instrument for this study was a structured survey questionnaire divided into four sections. The first section collected data on the socio-economic profile of respondents, including age, sex, income level, and employment status. The second section assessed cyber security concerns related to online shopping, focusing on issues like data usage, consent, and security measures. The third section measured the extent of e-commerce platform usage. The final section evaluated personal risk mitigation practices, such as using secure payment methods and checking for website security. The questionnaire underwent content validity testing to ensure relevance and clarity, and reliability was confirmed through the Kaiser-Meyer-Olkin (KMO) test, ensuring the instrument was both valid and reliable for the study.

TABLE 1. Kaiser-Meyer-Olkin (KMO) Reliability of Constructs (15 Cohorts)

Variable	*α*	N of Items	Internal Consistency
Level of E-Commerce Platform Usage	0.712	1	Acceptable
Cyber Security Concerns			
Data Usage	0.804	5	Good
Consent and Transparency	0.828	5	Good
Security Measures	0.816	5	Good
Personal Risk Mitigation			
Personal Risk Mitigation	0.756	5	Acceptable

TABLE 2. 5-Point Likert Scale used for the Survey Instrument

Scale	Mean Range	Description	Intensity
1	1.00-.1.8	Strongly Disagree	Very high Level
2	1.81- 2.60	Disagree	Low Level
3	2.61-3.40	Neutral	Average
4	3.41-4.20	Agree	High Level
5	4.21-5.00	Strongly Agree	Very high Level

Source: (Diaz et al., 2023)

Data Gathering Procedure

Data collection for this study involved distributing a structured survey questionnaire to young professionals in Koronadal City, aged 18 to 35, who were actively engaged in online shopping. The survey was administered digitally to ensure convenience and maximize participation. Prior to distribution, participants were informed about the study's purpose, confidentiality, and their voluntary participation. The researcher carefully reviewed the completed questionnaires for accuracy and consistency before entering the data into statistical software for analysis. This approach ensured reliable and valid data for assessing the relationship between cyber security perceptions and online shopping behaviour.

Statistical Analysis and Treatment

For this study, various statistical techniques were applied to analyze the data based on the study's objectives.

Objective 1- To determine the socio-economic profile of the respondents, frequency and percentage distribution were used. This method allowed the researcher to categorize and quantify demographic data, such as age, sex, income level, and employment status, providing a clear overview of the sample population's characteristics.

Objectives 2, 3, and 4- To assess cyber security concerns, the level of e-commerce platform usage, and the extent of personal risk mitigation practices, weighted mean and standard deviation were utilized. The weighted mean allowed the researcher to calculate the average perception and behavior based on varying levels of importance or frequency, while the standard deviation provided insights into the variability and consistency of the responses within each of these categories.

Objective 5- To examine the relationship between cyber security perceptions and the level of e-commerce platform usage, simple linear regression was employed. This statistical method helped determine the strength and direction of the relationship between the two variables, providing a clear understanding of how cyber security concerns may influence online shopping behavior (level of E-commerce platform usage) among the young professionals in the study.

These statistical techniques ensured that the data were analysed comprehensively, allowing the researcher to draw meaningful conclusions about the relationship between cyber security perceptions and online shopping behavior (level of E-commerce platform usage).

Ethical Considerations

This study adhered to the ethical guidelines set by the Philippine Health Research Ethics Board (PHREB) and complied with data privacy laws. Before data collection, the researcher obtained informed consent from all participants, ensuring they were fully aware of the study's purpose, their voluntary participation, and their right to withdraw at any time without penalty. Participants were assured that their responses would be treated with confidentiality and anonymity. The data collected were securely stored and only accessible to the researcher for analysis, in compliance with the Data Privacy Act of 2012. Additionally, any potentially identifying information was omitted from the final data set to protect participants' privacy. These ethical measures were taken to ensure the integrity of the study and the protection of participants' rights throughout the research process.

Results and Discussions

TABLE 3. Profile-Age

Age	Frequency	Percent	Valid Percent	Cumulative Percent
23-26	24	35.3	35.3	35.3
27-30	26	38.2	38.2	73.5
31-35	18	26.5	26.5	100.0
Total	68	100.0	100.0	

Table 3 illustrates the age distribution of the young professional respondents in the study. The largest group consists of individuals aged 27-30 years, comprising 26 participants (38.2%). The next largest group is between the ages of 23-26, with 24 participants (35.3%). The remaining 18 participants (26.5%) fall within the 31-35 age range.

The cumulative percentage indicates that a significant portion (73.5%) of the respondents is aged between 23 and 30 years, highlighting that the study predominantly reflects the experiences and perspectives of young professionals in the early to mid-stages of their careers. This demographic is key to understanding their perceptions of cyber security and online shopping behaviour.

TABLE 4: Profile-Sex

Sex	Frequency	Percent	Valid Percent	Cumulative Percent
Male	35	51.5	51.5	51.5
Female	33	48.5	48.5	100.0
Total	68	100.0	100.0	

Table 4 presents the distribution of the ages of young professional respondents in the study. The majority of the participants fall within the age range of 27-30 years, with 26 individuals (38.2%) in this group. The second largest group is between 23-26 years, comprising 24 participants (35.3%). The remaining 18 participants (26.5%) are aged between 31-35 years.

The cumulative percentage shows that 73.5% of the respondents are between the ages of 23 and 30, indicating that the study predominantly involved younger young professionals. The distribution suggests a strong representation of individuals in the early stages of their professional careers, which is relevant to understanding the cyber security perceptions and online shopping behaviours of this demographic.

TABLE 5. Profile-Monthly Income Level

Income level	Frequency	Percent	Valid Percent	Cumulative Percent
Below 10,000	51	75.0	75.0	75.0
11,000 - 20,000	11	16.2	16.2	91.2
21,000 - 30,000	6	8.8	8.8	100.0
Total	68	100.0	100.0	

Table 5 presents the monthly income levels of the young professional respondents. The largest group, consisting of 51 participants (75.0%), reported an income level of below 10,000 pesos. The next largest group is composed of 11 participants (16.2%) who earn between 11,000 to 20,000 pesos per month. The smallest group, with 6 participants (8.8%), reported an income level ranging from 21,000 to 30,000 pesos per month.

The cumulative percentage shows that 91.2% of the respondents earn below 20,000 pesos monthly, indicating that the majority of young professionals in the study have lower to middle-income levels. This income distribution is important in understanding the potential impact of cyber security concerns and online shopping behaviors, as lower-income individuals may have different attitudes and practices regarding e-commerce platforms and security concerns.

TABLE 6. The Employment Status of the young professionals

Employment Status	Frequency	Percent	Valid Percent	Cumulative Percent
Employed	25	36.8	36.8	36.8
Self-employed	32	47.1	47.1	83.8
Unemployed	11	16.2	16.2	100.0
Total	68	100.0	100.0	

Table 6 shows the employment status of the young professional respondents. The largest group, comprising 32 participants (47.1%), reported being self-employed. The second largest group consists of 25 participants (36.8%) who are employed. The remaining 11 participants (16.2%) are unemployed.

The cumulative percentage indicates that 83.8% of the respondents are either self-employed or employed, which reflects a high level of professional engagement among the young professionals in the study.

TABLE 7. Cyber Security Concerns- Data Usage

Statement	Mean	Std. Deviation
Please rate your level of concern about the security of your personal data when making purchases on e-commerce platforms.	4.57	0.63
Please rate your level of concern about the security of your financial information (credit card details, bank account information) when making purchases on e-commerce platforms.	3.62	1.26
Please rate your level of concern about the security of your login credentials (username and password) when accessing e-commerce platforms.	3.49	1.13
Please rate your level of concern about the security of your browsing activity (search history, visited websites) when using e-commerce platforms.	3.25	1.19
Please rate your level of concern about the security of your personal information (name, address, contact details) when providing them on e-commerce platforms.	3.07	1.18
OVERALL	3.60	1.08

Table 7 presents the concerns young professionals have regarding data security on e-commerce platforms. The highest level of concern is associated with the security of personal data during purchases (mean = 4.57, SD = 0.63), which falls under the "Strongly Agree" category, indicating a very high level of concern. Concerns about financial information (mean = 3.62, SD = 1.26) and login credentials (mean = 3.49, SD = 1.13) also indicate a high level of concern, reflected by an "Agree" rating. In contrast, concerns about browsing activity (mean = 3.25, SD = 1.19) and personal information (mean = 3.07, SD = 1.18) are moderate, with responses leaning toward "Neutral" to "Agree." Overall, the mean of 3.60 (SD = 1.08) suggests a high level of concern about cyber security among young professionals, particularly regarding personal and financial data security.

TABLE 8. Cyber Security Concerns -Consent and Transparency

Statement	Mean	Std. Deviation
I am concerned about the security of my personal data when making purchases on e-commerce platforms.	3.34	1.18
I am concerned about the security of my financial information (credit card details, bank account information) when making purchases on e-commerce platforms.	3.06	1.43
I feel that e-commerce platforms should be more transparent about how they collect, use, and share my personal data.	2.87	0.98
I am concerned about the security of my login credentials (username and password) when accessing e-commerce platforms.	3.12	1.24
I believe that e-commerce platforms should obtain my explicit consent before collecting and using my personal data.	3.43	1.33
OVERALL	3.16	1.23

Table 8 presents young professionals' concerns about consent and transparency in e-commerce platforms. The highest concern is about the security of personal data (mean = 3.34, SD = 1.18), which falls in the "Agree" category, reflecting a moderate to high level of concern. Similarly, the concern regarding financial information (mean = 3.06, SD = 1.43) is moderately high, but falls within the "Neutral to Agree" range. Respondents also express moderate concern about the security of login credentials (mean = 3.12, SD = 1.24). However, the concern about transparency (mean = 2.87, SD = 0.98) is relatively lower, indicating that respondents are somewhat less concerned about how e-commerce platforms handle their personal data, though still noting the importance of transparency. The belief that platforms should obtain explicit consent (mean = 3.43, SD = 1.33) is moderately high, showing an expectation of greater control over personal data usage. The overall mean of 3.16 (SD = 1.23) suggests that young professionals have a moderate level of concern about consent and transparency practices in e-commerce.

TABLE 9. Cyber Security Concerns-Security Measures

Statement	Mean	Std. Deviation
The security measures implemented by e-commerce platforms are sufficient to protect my personal and financial information.	3.47	0.82
I am concerned about the possibility of my personal and financial information being hacked or stolen while using e-commerce platforms.	3.16	0.78
E-commerce platforms should regularly update their security systems to address new cyber threats and vulnerabilities.	3.07	0.72
I am confident in the ability of e-commerce platforms to detect and prevent unauthorized access to my account.	2.84	0.84
E-commerce platforms should provide clear information on the security measures they have in place to protect my personal and financial data.	3.68	1.57
OVERALL	3.24	0.95

Table 9 summarizes young professionals' concerns regarding security measures on e-commerce platforms. The highest concern is about the adequacy of security measures (mean = 3.47, SD = 0.82), which falls within the "Agree" range, suggesting a moderate to high level of confidence in the platform’s ability to protect personal and financial data. However, respondents express concern about the possibility of their data being hacked (mean = 3.16, SD = 0.78), which indicates a moderate level of worry, though it is less intense than concerns about security measures themselves. There is also a clear expectation for e-commerce platforms to regularly update their security systems (mean = 3.07, SD = 0.72) to address emerging threats. A slightly lower concern is expressed regarding the ability to detect unauthorized access (mean = 2.84, SD = 0.84), suggesting that some professionals have less confidence in the platforms' capacity to prevent breaches. The need for clear communication about security measures (mean = 3.68, SD = 1.57) received a relatively higher rating, reflecting an important concern for transparency. The overall mean of 3.24 (SD = 0.95) suggests that while respondents are moderately concerned about security measures, they also expect higher security standards and clearer communication from e-commerce platforms.

TABLE 10. Level of usage in E-commerce platforms

	N	Minimum	Maximum	Mean	Std. Deviation
I use e-commerce platforms frequently for purchasing products or services.	68	1.00	5.00	3.7647	1.18596
OVERALL	68				

Table 10 shows that respondents generally use e-commerce platforms with a mean score of 3.76, indicating moderate frequency of use. The standard deviation of 1.19 suggests some variation in how often individuals use these platforms, with most young professionals using them regularly for purchases.

TABLE 11. The level of personal risk mitigation practices of the young professional customers

Statement	Mean	Std. Deviation
I regularly update my passwords on e-commerce platforms.	3.62	0.96
I use two-factor authentication (2FA) when it's available on e-commerce platforms.	3.53	1.23
I am cautious about clicking on links or downloading files from unknown sources while shopping online.	3.82	0.98
I regularly check and review the privacy settings of my accounts on e-commerce platforms.	3.68	1.04
I am aware of and understand the potential cyber security risks associated with online shopping.	3.09	0.69
OVERALL	3.55	0.98

Table 11 shows the level of personal risk mitigation practices among young professional customers. The overall mean score of 3.55 indicates that, on average, respondents engage in moderate to high levels of personal risk mitigation practices while shopping on e-commerce platforms. Specifically, they are most cautious about clicking on unknown links (mean = 3.82), and they regularly update their passwords (mean = 3.62) and review privacy settings (mean = 3.68). However, their awareness of cyber security risks (mean = 3.09) is lower, suggesting that while they practice some level of caution, there is room for improvement in overall risk awareness and mitigation. The standard deviations indicate varied levels of responses, with some practices (like using two-factor authentication) showing more variation than others.

TABLE 12. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.297[a]	.18	.060	.66911

a. Predictors: (Constant), Cyber Security Concerns

Table 12 presents the model summary for the regression analysis, which examines the relationship between cyber security concerns and the level of e-commerce usage. The R value of 0.297 indicates a weak positive correlation between the predictors (cyber security concerns) and the dependent variable (e-commerce usage). The R Square value of 0.18 suggests that approximately 18% of the variation in the level of e-commerce usage can be explained by the cyber security concerns. The Adjusted R Square of 0.060 accounts for the degree of freedom, indicating that the model is not a strong fit for predicting the level of e-commerce usage based on cyber security concerns alone. Finally, the Standard Error of the Estimate (0.66911) suggests a moderate level of error in predicting the dependent variable.

TABLE 13. ANOVA Table

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	2.819	2	1.409	3.148	.050[b]
	Residual	29.101	65	.448		
	Total	31.920	67			

b. Predictors: (Constant), Cyber Security Concerns

Table 13 shows the ANOVA results for the regression model analyzing the relationship between cyber security concerns and the level of e-commerce usage. The F-statistic of 3.148 indicates the overall fit of the model. The p-value (Sig.) of 0.050 suggests that the relationship between cyber security concerns and e-commerce usage is statistically significant at the 0.05 level, albeit marginally. This implies that cyber security concerns have a meaningful impact on the level of e-commerce usage, supporting the relevance of the model while highlighting its limited explanatory power.

TABLE 14. Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	Constant	1.877	.915		2.052	.044
	Cyber Security Concerns	-0.179	.088	.242	2.037	.046

Table 14 presents the coefficients for the regression model examining the influence of cyber security concerns on the level of e-commerce usage. The constant (B = 1.877, p = 0.044) indicates the baseline level of e-commerce usage when cyber security concerns are not considered. The coefficient for cyber security concerns (B = -0.179, p = 0.046) suggests a statistically significant but inverse relationship. Specifically, as concerns about cyber security increase, the level of e-commerce usage slightly decreases. This finding highlights the importance of addressing cyber security issues to encourage greater use of e-commerce platforms.

Conclusion

This study assessed the relationship between young professionals' perceptions of cyber security and their level of online shopping on e-commerce platforms in Koronadal City. The research objectives were successfully addressed, providing valuable insights into the factors influencing e-commerce usage in this demographic. Regarding the socio-economic profile, the study revealed that most young professionals in the sample were between 27 and 30 years old, earning below PHP 10,000 monthly, with a significant proportion being self-employed. These findings suggest a tech-savvy yet financially cautious group, which may influence their views on cyber security.

The study found that cyber security concerns, particularly regarding personal data security, were high among the respondents. These concerns were found to impact their level of engagement with e-commerce platforms, as higher concerns led to cautious usage patterns. The participants in the study reported moderate usage of e-commerce platforms, indicating that while online shopping is gaining traction, security concerns may limit more frequent engagement. Regarding personal risk mitigation practices, participants showed a moderate level of caution, such as regularly updating passwords and being wary of suspicious links, but the adoption of practices like two-factor authentication was not consistent.

The regression analysis revealed a significant inverse relationship between cyber security concerns and the level of e-commerce usage, indicating that as concerns about cyber security increase, the frequency of online shopping decreases. The ANOVA results further supported this significant relationship. These findings have significant implications for both e-commerce platforms and cyber security policy. E-commerce businesses should prioritize improving security measures and ensuring transparency regarding data usage and consent processes to address these concerns and encourage more frequent usage. Additionally, the study highlights the importance of educating young professionals on best practices for personal risk mitigation, such as enabling two-factor authentication and regularly reviewing privacy settings.

From a policy perspective, initiatives that raise awareness about cyber security risks in e-commerce could help reduce vulnerabilities and improve consumer confidence. Furthermore, understanding the socio-economic characteristics of this demographic such as their lower income levels and self-employment status can inform targeted cyber security interventions. In conclusion, while cyber security concerns significantly impact the online shopping behaviours of young professionals, addressing these concerns through effective security measures and user education could enhance the e-commerce experience and increase usage in Koronadal City.

References

Chellappa, R., & Pavlou, P. (2022). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368. https://doi.org/10.1108/09576050210447046

Davis, F., Gnanasekar, M., & Parayitam, S. (2021). Trust and product as moderators in online shopping behavior: Evidence from India. *South Asian Journal of Marketing,* 2(1), 28-50. . https://doi.org/10.1108/SAJM-02-2021-0017

Diaz, J., Abang, M., Atam, M., & Ballados, M. (2023). Vicenarian professionals' awareness and determinants of engagement in cryptocurrency in Koronadal City, South Cotabato, Philippines. *Journal of Applied Management and Business 4*(2). https://doi.org/10.37802/jamb.v4i2.437

Haddad, G., Shahab, A., & Aïmeur, E. (2018). Exploring user behavior and cybersecurity knowledge: An experimental study in online shopping. *16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1-10). https://doi.org/10.1109/PST.2018.8514190

Kedah, Z. (2023). Use of e-commerce in the world of business. *Startupreneur Business Digital (SABDA Journal), 2*(1). https://doi.org/10.33050/sabda.v2i1.273

Kim, Y., & Vonortas, N. (2018). Managing risk in the formative years: Evidence from young enterprises in Europe. *Technovation, 34,* 454-465. https://doi.org/10.1016/J.TECHNOVATION.2014.05.004

Omar, S., Kovalan, K., & Bolong, J. (2020). Information security awareness among youth in Klang Valley: A focus group discussion. *The International Journal of Academic Research in Business and Social Sciences, 10,* 193-205. https://doi.org/10.6007/IJARBSS/V10-I16/8302

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Tarhini, A., Alalwan, A., Al-Qirim, N., Algharabat, R., & Masa'deh, R. (2018). An analysis of the factors influencing the adoption of online shopping. *International Journal of Technology Diffusion, 9,* 68-87. https://doi.org/10.4018/IJTD.2018070105

Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A., Zhanseitov, A., & Jumabaeva, S. (2020). Features of e-commerce risk management in modern conditions. *Academy of Strategic Management Journal, 19*(1). https://www.abacademies.org/articles/Features-of-e-commerce-risk-management-in-modern-conditions-1939-6104-19-1-515.pdf

Wallang, M., Shariffuddin, M., & Mokhtar, M. (2022). Cyber security in small and medium enterprises (SMEs). *Journal of Governance and Development (JGD), 18*(1), 75–87. https://doi.org/10.32890/jgd2022.18.1.5