Advances in Consumer Research
https://acr-journal.com/

Volume-2 | Issue-1 | Jan-Feb 2025

Original Researcher Article

Culture and Cybersecurity ’s Role in the Continual Usage of E-Commerce Platforms in Sub-Saharan Africa: Perspectives from Ghana

Felicia Naatu[1], Stephen Naatu[1], Théophile Bindeouè Nassè[1]

[1]SDD University of Business and Integrated Development Studies, Ghana

Received: 05 Nov 2024
Revised: 27 Nov 2024
Accepted: 25 Dec 2024
Published: 14 Jan 2025

Abstract

Cybercrimes such as phishing, hacking, identity theft, fraud, and misrepresentation are increasingly eroding consumer confidence in e-commerce across Sub-Saharan Africa. As a result, Cybersecurity has become a critical concern for businesses, consumers, and governments. This study examines the relationship between Cybersecurity, Uncertainty Avoidance, Digital Trust, and the Continual Usage of e-commerce platforms among consumers in Ghana. Using structural equation modeling, the study reveals that Cybersecurity significantly influences Continual Usage, Uncertainty Avoidance, and ICT Skills. It also finds that Uncertainty Avoidance mediates the relationship between Cybersecurity and Digital Trust, while ICT Skills mediate the relationship between Cybersecurity and Continual Usage. Furthermore, Uncertainty Avoidance, Digital Trust, and ICT Skills collectively explain the relationship between Cybersecurity and Continual Usage of e-commerce platforms. The findings emphasize the need for strong Cybersecurity measures with user-friendly features, user training to enhance ICT Skills, and effective regulatory policies to reduce uncertainty among the risk-averse consumers. This approach encourages greater adoption of e-commerce while mitigating the risks of cyberattacks. The insights have practical implications for e-commerce businesses, policymakers, and individuals, highlighting the importance of Cybersecurity in building Digital Trust and fostering Continual Usage. The study contributes to the existing literature by underscoring the critical role of Cybersecurity in cultivating consumer trust and loyalty within the e-commerce sector.

Keywords: Cybersecurity, Digital Trust, ICT Skills, E-commerce, Continual Usage

INTRODUCTION

In today's digital age, online buying and selling of goods and services known as electronic commerce or e-commerce have become integral to global commerce, offering convenience, accessibility, and a wide range of services to users worldwide (Naatu et al., 2024; Oguta, 2024). This current global culture accelerated when measures aimed at curbing the transmission of COVID-19 were implemented to limit human interaction (Florea et al., 2022). As the reliance on these platforms grows, so does the need for robust information security practices to protect both businesses and consumers from cybercrime which is also on the increase (Gangwer and Narang, 2021; Azizah, 2021; Ogar, 2022). While the people of Sub-Saharan Africa are trying to adopt digital technology platforms, most of them lack information and communication technology (ICT) skills (Ogar, 2022). This vulnerability makes it easier for cybercriminals to exploit, especially since even experts have been reported to struggle with detecting cyberattacks—let alone individuals with limited technical knowledge (Ogar, 2022). For instance, e-commerce platforms often gather sensitive information including names, addresses, and payment details of consumers (Oguta, 2024). As a result, despite the growing role of e-commerce as an essential technology, many people remain distrustful and insecure about engaging in online transactions (Alzoubi et al., 2022). This coupled with the fact that technology adoption does not occur in cultural vacuum has led to disparities in the adoption and usage rate of emerging technologies in different cultural contexts (Oregon et al., 2008).

Culture profoundly influences how individuals perceive, adopt, and interact with each other (Okello et al., 2019). Cultural values, norms, and practices shape attitudes toward innovation, risk, and change which can either accelerate or hinder the adoption of new technologies (Okello et al., 2019; Altuncu et al., 2012). For example, in cultures that emphasize collectivism, individuals often are more open to connectivity and collaboration (Naatu et al., 2020; Okello et al., 2019). Thus, they are likely to encourage their peers, family and friends to adopt digital platforms that can help them connect. In contrast, cultures that value individualism and autonomy might prioritize technologies that offer personal control or privacy. The cultural dimension, Uncertainty Avoidance, is identified to be an influential element on individual

acceptance and patronage of products and services (Sartono et al., 2024). For instance, high sense of Uncertainty Avoidance may influence a person's trust and even their patronage of some products or services (Sartono et al., 2024).

Studies exploring the effect of Cybersecurity and cultural factors on Continual Usage of e-commerce platforms are limited in Sub-Saharan Africa. Most research have focused on aspects such as information security and consumer trust (e.g., Pieters, 2011; Barnard & Wesson, 2014), the relationship between usability and trust in information systems (Sasse, 2005), and how trust impacts the ongoing use of e-commerce platforms (Pinem et al., 2018). No study has simultaneously examined the effect of Cybersecurity on Culture, particularly Uncertainty Avoidance—and Digital Trust in e-commerce platforms. As noted by Sasse (2005) and Ghelani (2022), despite the availability of numerous security mechanisms in cyberspace (e.g., Akiddo, New Relic, and Rippling IT), many users find them overly complex, especially in regions with high illiteracy rates, widespread poverty, weak institutions, and poor infrastructure such as Sub-Saharan Africa (Alkhwaldi et al., 2023; Naatu et al., 2023).

This study seeks to explore the impact of Cybersecurity on Continual Usage of e-commerce platforms, Uncertainty Avoidance, Digital Trust and ICT Skills (i.e. how individuals leverage their ICT abilities for online shopping and selling) using the Social Exchange Theory. The research questions are:

1. What is the effect of Cybersecurity on Uncertainty Avoidance, Digital Trust in e-commerce technology platforms and the Continual Usage of e-commerce platforms?
2. Do ICT Skills, Digital Trust and Uncertainty Avoidance mediate the relationship between Cybersecurity and Continual Usage of e-commerce platforms?

Using Social exchange theory, the study discusses the factors that build trust in business transactions. We posit that Cybersecurity directly impacts on Uncertainty Avoidance, ICT Skills and Continual Usage of e-commerce platforms. We also posit that, Uncertainty Avoidance, Digital Trust, and ICT Skills mediates the relationship between Cybersecurity and Continual Usage of e-commerce platforms. This study is essential for bridging gaps in existing literature as it offers valuable insights into the factors shaping consumer behaviour in the digital landscape of Sub-Saharan Africa, Ghana. It provides critical market intelligence for businesses and serves as a foundation for future research and policy formulation.

The structure of the study is as follows: it begins with a review of relevant literature and the theoretical framework, followed by the development of hypotheses. The methodology is then outlined, before presentation and discussion of the results. The study concludes with a summary of the findings and their implications.

LITERATURE REVIEW

E-commerce, or electronic commerce, refers to the digital transformation of traditional commerce which allows the transaction of businesses online using information technology, Internet, computer, and other electronic devices (Oguta, 2024). It plays a vital role in industrial and economic growth, offering efficient, convenient, and fast business processes (Babu et al., 2020). It enables businesses and individuals to buy and sell goods and services online (Tofan & Bostan, 2022). E-commerce operates across various devices, including computers, tablets, smartphones, and other smart gadgets (Tofan & Bostan, 2022). Activities in e-commerce entails online payments, sales, advertising, and browsing (Kinal, 2022). Some platforms function through mobile apps, while others rely on traditional websites for transactions. Leading e-commerce businesses today include Jumia, Kikuu, and Amazon (Alkhunaizan & Ali, 2022).

The driving force behind e-commerce is the digital economy also known as the internet or web economy, which relies on digital technologies, especially, the internet (Pomeroy, 2020). In recent years, the growth of the digital economy has led to a significant increase in e-commerce users in Sub-Saharan Africa. This surge marks a major shift from the late 1990s when internet access in Africa was a luxury limited to a few (Interpol African Cyberthreat Assessment Report, 2024). The rise in e-commerce has been fueled by factors such as the COVID-19 pandemic and the African Continental Free Trade Area (AfCFTA) agreement which has reduced trade barriers among African nations (Han et al., 2023). Consequently, the number of e-commerce customers have skyrocketed, and a range of new e-products and services emerged, allowing consumers to shop conveniently from home (Alkhunaizan & Ali, 2022).

Alongside this rapid growth, there has been a growing concern regarding the rise in cybercrime. As technology advances, cybercriminals have developed highly sophisticated methods to exploit vulnerabilities (Interpol African Cyberthreat Assessment Report, 2024; Shakeri et al., 2022). Cybercrime is the term used to define a broad range of illegal behaviours that involve using digital equipments or networks (Sartono et al., 2024). Victims of cybercrime face financial, psychological, and emotional harm. Cybercrime affects individuals, governments, and businesses alike, explaining the variety of security measures in place to protect cyberspace (Sartono et al., 2024). Online security or Cybersecurity is a type of information system security

which involves processes and practices designed to detect, prevent, and ensure safety on the internet (Rajaonah, 2017). Cybersecurity encompasses key principles such as confidentiality, integrity, availability, authentication, and non-repudiation (Shakeri et al., 2022). Cybersecurity is different from the information security which is broad and involves protecting all types of information, regardless of whether it's stored on digital devices or in other forms, such as paper records (Shakeri et al., 2022).

For e-commerce platforms to be successfully embraced, they must earn users' trust to encourage ongoing use, hence the need for Cybersecurity (Sartono et al., 2024; Oguta, 2024). The literature defines trust as a firm believe in the reliability or capability of a system or entity (Oguta, 2024; Liu et al., 2022). It entails confidence that a system can deliver consistent, dependable results, and is characterized by positive relationships, sound judgment, expertise, and minimal risk exposure (Oguta, 2024).

Culture also plays a vital role in consumers ability to adopt, use and continue using technologies (Alkhwaldi et al., 2023). Hofstede's (1991) study identifies four dimensions in which people from different cultures differ. One of the dimensions is Uncertainty Avoidance (Hofstede, 1991). This dimension is closely related to an individual's attitude toward risk and uncertainty. Specifically, it refers to the extent to which people feel threatened by and attempt to avoid uncertainty and ambiguity (Hofstede, 2001). In cultures with high Uncertainty Avoidance, individuals often view unfamiliar or unpredictable situations as threatening. Consequently, they tend to seek clarity and clear interpretations of events in both their personal relationships and business dealings, often searching for products or services that provide certainty and reliability (Hofstede, 2001).

However, while a wide range of Cybersecurity systems are available, many are perceived as difficult to use (Sasse, 2005; Familoni, 2024), highlighting the importance of user-friendliness for the adoption and continued use of e-commerce technologies. As Sartono et al. (2024) observed, complex technologies can introduce uncertainty, which may influence individuals' decisions to adopt or persist in using a technology. This suggests a critical link between Cybersecurity , Digit Trust, Uncertainty Avoidance, ICT Skills, and the Continual Usage of e-commerce platforms. These relationships however remain underexplored in Sub-Saharan Africa.

Research on Cybersecurity has been explored from various perspectives. For example, Rajaonah (2017) reviewed studies on trust in information system security, particularly concerning infrastructure protection, while Sartono et al. (2024) conducted an empirical analysis of the impact of sustainable digital transformation on the perceived value and adoption of Industry 4.0 in Indonesia. Other notable studies include a literature review on security challenges in cyberspace (Oguta, 2024), an empirical analysis of user acceptance and satisfaction in e-commerce (Kassim et al., 2012), and an exploration of how providing security system information influences user trust (Pieters, 2011). Pinem et al. (2018) examined the role of trust in the continued use of government-to-business online services. However, to the best of our knowledge, no study has specifically investigated how Cybersecurity affects Uncertainty Avoidance, Digital Trust, and the Continual Usage of e-commerce platforms.

Our study aims to address this gap by exploring these key influencing factors of e-commerce on Continual Usage. Cybersystems security challenges can have dire consequences, affecting critical services and their usage (Sartono et al., 2024; Familoni, 2024), hence, research in this area would be highly important. The findings will expand the current body of knowledge and provide valuable insights for stakeholders and practitioners within the e-commerce industry.e

2.1 Theoretical review

Research across multiple disciplines, including psychology, economics, marketing, and management information systems, have proposed a range of theories to explain trust (Thurik et al., 2023). One prominent theory is Rational Choice Theory. This theory suggests that trust is based on a logical evaluation of the costs and benefits involved in trusting others (Trabucchi et al., 2023). Another influential framework is the Diffusion of Innovations Theory, which focuses on trust in the context of adopting new ideas, products, or technologies. According to this theory, individuals are more likely to trust and embrace innovations when they perceive them to align with their existing values, beliefs, and social norms (Ullah et al., 2021).

In our study, we draw on Social Exchange Theory to explain the dynamics that shape individual trust in business interactions. Building on the concepts of Rational Choice Theory, Social Exchange Theory suggests that trust develops through ongoing social exchanges between individuals (Park & Kim, 2023). This theory views trust as a reciprocal process, where people base their trust on past experiences and the expectation of future benefits. It is frequently applied to analyze various forms of social relationships, such as business relationships, families, romantic partnerships, friendships, and social networks (Chapman et al., 2022). Social Exchange Theory offers valuable insights into how individuals navigate relationships, negotiate power dynamics, and evaluate the balance of rewards and costs. It sheds light on factors influencing attraction, consumer satisfaction, commitment, and trust in relationships, as

well as decision-making in social interactions such as internet business transactions (Lauren et al., 2021).

2.2. Hypotheses Development

The main variables of the study are: Cybersecurity (CS), Uncertainty Avoidance (UA), Digital Trust (TR), Information and Communication Technology Skills (ICT Skills), and Continual Usage (CU) of e-commerce platforms.

2.2.1 Cybersecurity (CS)

Despite the growing importance of e-commerce, concerns over cyber theft, fraud, forgery, hacking, harassment, and other forms of cyberattacks have left many users hesitant to engage with online platforms (Solms & Solms, 2018). This apprehension is primarily due to e-commerce platforms' collection of sensitive information such as names, addresses, and payment details, which heightens fears around data privacy and security (Oguta, 2024). As a result, security has become a crucial factor in e-commerce (Oguta, 2024).

Cybersecurity and information security both play vital roles in protecting valuable data, yet, they address different aspects despite often being used interchangeably (Solms & Solms, 2018). Cybersecurity specifically focuses on safeguarding computer systems and networks from malicious actors seeking to breach or disrupt them (Rajaonah, 2017; Oguta, 2024). This includes efforts to prevent, detect, and respond to threats such as hacking and malware, while also ensuring the security of websites and digital platforms. In contrast, information security has a broader focus, aiming to protect all types of information, whether stored digitally or in physical formats, such as paper records (Solms & Solms, 2018).

Several studies, including Kassim and Abdullah (2010), emphasize that Cybersecurity is a critical prerequisite for the adoption and use of e-commerce platforms and services. According to Oguta (2024) Cybersecurity is essential for fostering trust among internet users (Oguta, 2024). Similarly, Löbbers and Benlian (2019) affirm that robust Cybersecurity positively influences individual confidence and trust in digital platforms, it allows them to continue using the platforms. Based on the above we argue that strong Cybersecurity is essential for fostering trust among internet users, encouraging them to engage with and to continue using e-commerce platforms. Therefore we hyposize that:

H_1: *Cybersecurity positively influences e-commerce platforms Continual usage*.

2.2.4 Uncertainty Avoidance

Uncertainty is an individual's perceived inability to accurately predict an outcome or situation (Altuncu et al., 2012). It is often experienced as a state of not knowing something about ourselves or our environment, which makes it difficult to prepare for or cope with the unknown (Altuncu et al., 2012; Alkhwaldi et al., 2023). Uncertainty Avoidance, a concept from Hofstede's (1991) cultural dimensions, refers to the extent to which individuals in a society feel threatened by uncertainty and ambiguity and take steps to avoid it (Alkhwaldi et al., 2023). Culture, in this context, refers to the collective mindset of a group of people within a specific community or society, which shapes their behaviour and distinguishes them from others (Alkhwaldi et al., 2023). In societies with low Uncertainty Avoidance, the need for security is relatively low, and people tend to accept life as it comes. These cultures are more likely to embrace new situations, diverse viewpoints, and various technologies even if they are complex or uncertain (Alkhwaldi et al., 2023).

On the other hand, high Uncertainty Avoidance cultures are characterized by a higher need for security (Altuncu et al., 2012). In these societies, individuals are more cautious and seek security measures, clear guidelines, rules, and predictable outcomes (Altuncu et al., 2012; Alkhwaldi et al., 2023). People in these cultures tend to prefer certainty and stability over ambiguity. Thus, Cybersecurity may eradicate uncertainty and minimise individual's fear of cyber attack in e-commerce, gain their trust and lead to continual usage of e-commerce platforms. Based on the argument above, we hypothesize that:

H_2: *Cybersecurity is significantly related to Uncertainty Avoidance (UA)*

2.2.2 Digital Trust (DT)

Digital Trust refers to an individual's confidence in the safety, privacy, security, reliability, and ethical handling of their personal data by companies in the digital environment (Oguta, 2024). It is closely linked to the perceived value of the information exchanged (Sartono et al., 2024). In the context of e-commerce, Digital Trust reflects the confidence customers place in platforms to meet their needs, deliver positive experiences, and protect their personal information. This trust is essential for the long-term success and growth of e-commerce businesses. As Valencia-Martinez et al. (2023) showed, trust has a direct impact on users' intentions to engage with e-commerce platforms and serves as a key indicator of perceived security, which supports the hypothesis of this research. Furthermore, Saeed (2019) showed that Cybersecurity significantly enhances consumer satisfaction and trust in e-commerce, emphasizing the important role security plays in fostering trust. This research aligns with those findings, asserting that Cybersecurity positively influences Digital Trust. Hence we hypothesize that:

H_3: *Uncertainty Avoidance has a significant positive effect on Digital Trust*

2.2.3 Continual Usage (CU)

Continual Usage refers to an individual's intention to use a technology or platform now and in the future

(Rahmayanti et al., 2022; Menon, 2022). It reflects a individual's decision to adopt and continue using a particular product or service both now and in the future (Menon, 2022). In this study context, Continual Usage implies that if individuals feel assured that the e-commerce platform they are using is easy to navigate, free from fraud, and secure, it enhances their trust in the e-commerce process and platform. This may in turn motivate them to keep using the platform in the future. Trust, in this case, refers to the confidence individuals have that a process or system will function successfully. As e-commerce users' trust in the reliability and security of the platforms growth, this will likely lead to Continual Usage. This hypothesis is supported by Darmiasih and Setiawan (2020). The study hypothesizes that:

H_4: *Digital Trust positively influences the Continual Usage of e-commerce service platforms*

H_5: *The relationship between Cybersecurity and Digital Trust is mediated by Uncertainty Avoidance.*

2.2.4 Information and communication technology skills (ICT Skills)

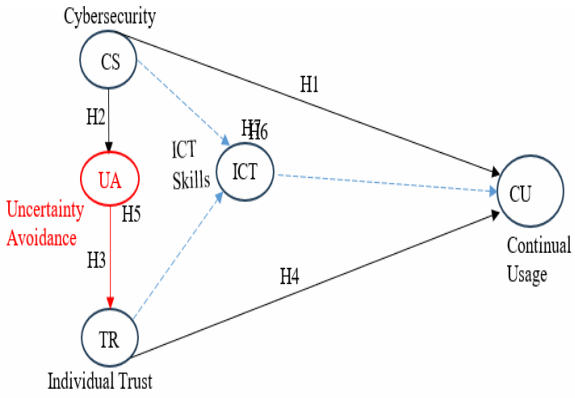
ICT skill refers to the basic computer and internet skills for operating, processing, and dissemination of information including changing, accessing and using software and hardware of computer and internet devices. The ability to detect and solve problems of ICT and knowledge in digital surroundings is often attributed to the extent of ICT Skills a person has or has not (Adams & Alhassan, 2021). ICT Skills are crucial for managing information security and effectively using e-commerce platforms (Thomas, 2018). While cyberfraud may sometimes go unnoticed by even experts or individuals well-versed in information technology, those with ICT Skills are generally more capable of detecting and avoiding cyberattacks compared to those without such skills (Ben-Asher & Gonzalez, 2015). As a result, individuals with ICT knowledge are at relatively lower risk of falling victims to fraud. In contrast, individuals who lack ICT Skills are more vulnerable to fraud as they may fail to recognize cyberattacks or potential threats to information systems (Ben-Asher & Gonzalez, 2015). Research shows that people without ICT expertise are significantly more likely to become victims of fraud (Xu et al., 2022).

Moreover, ICT Skills are essential in moderating the relationship between personal trust and the continued use of e-commerce platforms (Amofah, 2022). Individuals with strong ICT Skills are better positioned to build trust and maintain their use of these platforms. A solid understanding of information and communication technologies enhances users' confidence in the security and reliability of e-commerce services. Research indicates that familiarity with a system or process is vital for fostering trust (Rezaei & Bresciani, 2020). As such, ICT Skills play a crucial role in shaping the link between personal trust and sustained engagement with e-commerce platforms. Those with ICT expertise are more adept at recognizing fraudulent alerts or security threats, enabling them to navigate platforms with greater ease and avoid cyberattacks. This ability to detect and mitigate risks not only strengthens their trust in the platform but also boosts their willingness to continue using e-commerce services. Based on this, we hypothesize that:

H_6: *The relationship between Cybersecurity and Continual Usage of e-commerce platforms is significantly mediated by ICT Skills.*

H_7: *Uncertainty Avoidance, Digital Trust and ICT Skills are significant mediators of the relationship between Cybersecurity and Continual Usage of e-commerce platforms*

Below is the study model showing the hypotheses from hypothesis 1 to hypothesis 9.



(Source: Authors' Construct, 2023).

METHODOLOGY

The study investigates the impact of Cybersecurity and Digital Trust, ICT Skills, and Uncertainty Avoidance on the Continual Usage of e-commerce among Ghanaians. Ghana, a Sub-Saharan African country presents a fascinating context for this research due to its progress in internet and digital technology adoption despite facing economic, institutional, and infrastructural challenges. The majority of Ghanaians possess limited ICT Skills, making this setting uniquely relevant and intriguing for exploring the causal relationship among these factors and e-commerce platform usage.

Research design: A quantitative research design was used to facilitate a rigorous and objective analysis (Naatu et al., 2024) and measurement acuracy for more precise results (Nassè, 2018) . The study employed a convenience sampling strategy, selecting respondents who were readily available and willing to participate. While this approach limits the ability to generalize the findings, it offers several advantages such as being less time-consuming and cost-effective (Fricker & Schonlau, 2002). The challenge of securing voluntary participation further justified the use of convenience sampling as the

primary method for gathering responses (Naatu et al., 2024). The data collection was conducted between April 2023 and April 2024. To get participants who were genuinely interested and willing to voluntarily participate in the survey, we assured them of anonymity and avoided enticing them with gifts for participation. This helped to prevent speed answers (Naatu et al. 2022). Data collection was organized by dividing the country into three regions: the Southern, Middle, and Northern belts. Three agents were assigned to each region to distribute the questionnaires and gather responses. Initially, 117 responses were collected, with 38 from the Southern belt, 10 from the Middle belt, and 69 from the Northern belt. However, 7 responses from the Southern belt, 3 from the Middle belt, and 7 from the Northern belt were incomplete, resulting in the removal of 17 responses. This left a final total of 100 usable responses.

To determine an appropriate sample size, the study followed the "10-times rule" for Partial Least Squares Structural Equation Modeling (PLS-SEM), a widely accepted guideline for estimating the minimum sample size (Hair et al., 2011). According to this rule, the sample size should exceed 10 times the number of inner and outer model connections (Goodhue et al., 2012). Since each of the study's constructs—Cybersecurity , Digital Trust, ICT Skills, Uncertainty Avoidance, and Continued Usage—were represented by five indicators, the minimum required sample size was calculated to be 50 (i.e., 5 indicators × 10). However, the actual sample size surpassed this requirement, with 117 responses initially collected, and 100 responses deemed valid and complete, providing a solid basis for analysis, as shown in Table 1. The respondents were individuals aged 18 and older, all of whom could read and write. Their educational backgrounds ranged from senior secondary school to PhD levels. They were selected based on their ability to comprehend and respond appropriately to the survey questions (Naatu et al., 2024). Of the respondents, 85% were single, while 15% were married (see details in Table 1).

Table 1. Demographic Distribution of Respondents

Demographic	Characteristics	Number	Percentage
Gender	Male	67	67
	Female	33	33
	Total	100	100
Age	18 -25years	58	58
	36-45years	25	25
	46-55years	17	17
	Above 55years	0	0
	Total	100	100
Education	SHS	8	8
	Degree	75	75
	Masters	16	16
	PhD	1	1
	Total	100	100
Marital Status	Single	85	85
	Married	15	15
	Total	100	100
Monthly Income	GHC 0-GHC1000	69	69
	GHC 1001-	19	19
	GHC2000 above	12	12
	Total	100	100
Occupation	Student	62	62
	Entrepreneur	11	11
	public servant	17	17
	private/NGOs	10	10
	Total	100	100
Location	Southern belt	31	31
	Middle belt	7	7
	Northern belt	62	62
	Total	100	100

(Source: Authors' Construct, 2023)

4.Measurement Items

A four-step process was followed based on Li et al. (2018) to ensure the reliability and validity of the constructs. The steps included item generation, pilot testing (preliminary study), a full preliminary study, and finally, a comprehensive analysis of the hypothesized model. Items for the constructs were derived from previous literature. Items measuring Cybersecurity (CS) were adapted from Calder et al. (2009), ICT Skills from Rezaei and Bresciani (2020), Digital Trust (TR) and Continual Usage from Nambisan and Baron (2007), while Uncertainty Avoidance was taken from (Altuncu et al., 2012). Each construct was assessed using a 5-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Indicator reliability refers to the degree to which a factor explains the variance in the data. This was assessed using reflective factor loadings, which range from 0 to 1. A loading of 0.7 or higher is considered acceptable, while values below 0.7 are regarded problematic. Items with loadings below this threshold were excluded from the analysis. For example, item 1 (0.193), 3 (0.249), and 4 (0.401) from the Cybersecurity (CS) construct were removed, leaving items 2 and 5, which demonstrated adequate indicator reliability. Additionally, item 3 from the ICT Skills construct and item 2 from the Uncertainty Avoidance (UA) construct were also discarded (see details in Table 2). All remaining factor loadings were within the recommended range.

Table 2. Factor Loadings

Indicator item Cross-loading/factor loadings

Variable	Continual Usage	Information Security	ICT Skills	Individual Trust	Uncertainty Avoidance
CU1	0.704				
CU2	0.757				
CU3	0.934				
CU4	0.858				
CU5	0.888				
CS1		Dropped			
CS2		0.838			
CS3		Dropped			
CS4		Dropped			
CS5		0.879			
ICT1			0.920		
ICT2			0.928		
ICT3			Dropped		
ICT4			0.852		
ICT5			0.897		
TR1				0.890	
TR2				0.890	
TR3				0.919	
TR4				0.925	
TR5				0.879	
UA1					0.760
UA2					Dropped
UA3					0.784
UA4					0.804
UA5					0.711

Note: The threshold of Indicator loadings is ≥ 0.708

(Source: Authors' Construct, 2023)

To determine the internal consistency of the constructs, Cronbach alphas (α), Rho A, Composite reliability and Average variance extacted (AVE) were also used. The recommended threshold for Cronbach alphas (α), Rho A, and Composite reliability is 0.7. For the AVE, 0.50 is the minimum threshold. As shown in Table 3., all were above the minimum recommended thresholds. The Cronbach alphas (α) ranged from 0.700 to 0.942, Rho A from 0.700 to 0.943, and Composite Reliability from 0.849 to 0.956. The AVE ranged between 0.568 to 0.811 (See details in Table 3).

Table 3. Construct Reliability

Variable	Cronbach Alpha (α)	Rho A	Composite Reliability	Average variance extracted (AVE)
Continual Usage	0.887	0.908	0.918	0.693
ICT Skills	0.921	0.931	0.944	0.809
Digital Trust	0.942	0.943	0.956	0.811
Cybersecurity	0.700	0.700	0.849	0.738
Uncertainty Avoidance	0.748	0.752	0.840	0.568

Note: The threshold of Cronbach's Alpha, Composite Reliability is ≥ 0.7, and (AVE) is ≥ 0.5
(Source: Authors' Construct, 2023)

Table 4. Discriminant Validity- Heterotrait-Monotrait Ratio (HTMT)

Variable	Continual usage	ICT Skills	Individual trust	Cybersecurity	Uncertainty Avoidance
Contintual Usage	0.832				
ICT Skills	0.706	0.803			
Digital Trust	0.829	0.581	0.850	0.850	
Cybersecurity	0.800	0.621	0.810		
Uncertainty Avoidance	0.704	0.632	0.802	0.800	0.754

Note: None of the constructs should measure up to 90% or 0.90 against other constructs. Also, The √AVE (in bold) should be > than the factor correlations with each other.
(Source: Authors' Construct, 2023)

The study assessed the construct validity using measures of discriminant validity, specifically the Heterotrait-Monotrait Ratio (HTMT). HTMT measures the differentiation between a variable and other variables in a study. Henseler et al., (2015) argue that, unlike other measures such as the Fornell and Larcker, (1981) criterion, HTMT performs well in situations where the item loadings of constructs differ slightly. For valid discriminant validity, HTMT values close to zero shows good discriminant validity and scores above 0.85 shows there is a problem with discriminant validity. As Table 4 shows, the results shows sufficient fitness as they suggest that the items distinctively measure their assigned constructs (Henseler et al., 2015). HTMT values presented in Table 4 are below the threshold of 0.85. Also, the square root of the Average Variance Extracted (√AVE) should be greater than the factor correlations with each other (Naatu et al., 2024; Voorhees et al., 2016). The results confirm that we have no discriminant validity issues with the variables. This is evident in Table 4, where the √AVE values (in bold) are higher than the factor correlation values.

Table 5. SRMR

Variable	Original Sample (O)	Sample Mean (M)	95%	99%
Saturated Model	0.052	0.051	0.062	0.067
Estimated Model	0.073	0.066	0.074	0.070

Note: SRMR value of above 0.08 indicates the absence of fit.
(Source: Authors' Construct, 2023)

Table 6. Variance Inflation Factor (VIF)

	Cont. usage	ICT Skills	Ind. Trust
Continual Usage			
ICT Skills	1.496		
Digital Trust	1.921	1.681	
Cybersecurity	1.761	1.681	1.000

Note: 1 ≤ VIF < 5: are acceptable.
(Source: Authors' Construct, 2023)

5. SEM Estimation of Conceptual Model

The model's fitness was further assessed using SRMR (Standardized Root Mean Square Residual) estimations, as proposed by Hu and Bentler (1999). The SRMR score for the estimated was 0.073 is below the 0.08 threshold, indicating that there is no significant measurement or structural model misspecifications. This suggest that the model is well-fitting. Additionally, to assess potential collinearity issues, the study examined the Variance Inflation Factors (VIFs) (see Table 6). The VIF values ranged from 1.496 to 1.921, which indicates the absence of collinearity problems.

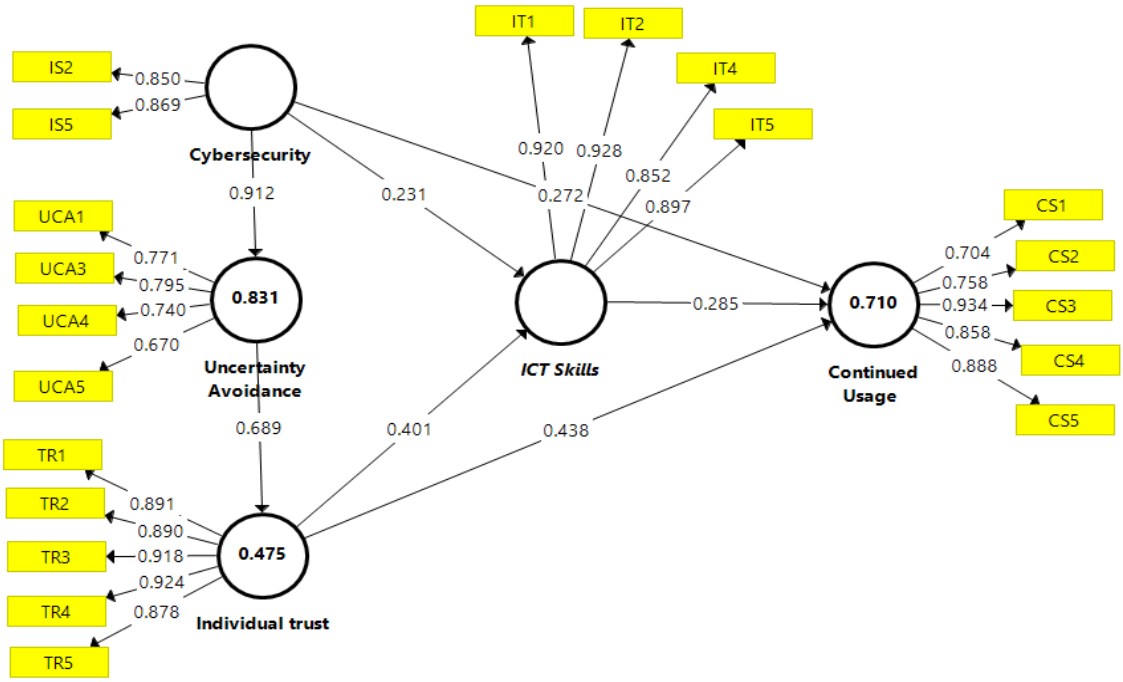


Fig2.Estimated model.
(Source: Authors' Construct, 2023)

MODEL 1.

Table 7. Direct Regression Results

	Path	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values	Confirmed
1.	CS -> CU	0.272	0.263	0.102	2.679	0.007	Yes
2.	CS -> UA	0.912	0.914	0.015	62.322	0.000	Yes
3.	UA -> TR	0.689	0.690	0.061	11.239	0.000	Yes
4.	TR -> CU	0.438	0.444	0.092	4.740	0.000	Yes
	CS -> ICT	0.231	0.235	0.108	2.145	0.032	Significant
	TR -> ICT	0.401	0.401	0.109	3.694	0.000	Significant
	ICT ->CU	0.285	0.288	0.066	4.347	0.000	Significant

Note: The threshold of, t- values ≥ 1.65, P-values < 0.05 at 95% confidence interval, Std beta > 0., IS = Information Security; CU = Continual usage; TR = Individual Trust; ICT = Information and communication technology skills.
(Source: Authors' Construct, 2023)

.

Table 7. Indirect Effect

	Path	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values	Confirmed
5.	CS -> UCA -> TR	0.628	0.631	0.056	11.129	0.000	Yes
	CS -> ICT -> CU	0.066	0.068	0.037	1.765	0.078	No
6.	TR -> ICT -> CU	0.114	0.115	0.041	2.772	0.006	Yes
	CS -> UA -> TR -> ICT	0.252	0.255	0.078	3.212	0.001	Significant
	CS -> UA -> TR -> CU	0.275	0.283	0.072	3.843	0.000	Significant
7.	CS -> UA -> TR -> ICT -> CU	0.072	0.073	0.027	2.625	0.009	Yes

	UA -> TR -> ICT -> CU	0.079	0.080	0.031	2.577	0.010	Significant
	UA -> TR -> CU	0.302	0.309	0.077	3.907	0.000	Significant
	UA -> TR -> ICT	0.276	0.279	0.087	3.166	0.002	Significant

Note: The threshold of, t-values ≥ 1.65, P-values < 0.10 at 90% confidence interval, Std beta > 0.

DISCUSSION AND RESULT

The study tested a total of seven hypotheses. First, we hypothesized that, Cybersecurity has a significant positive impact on the Continual Usage of e-commerce platforms. Secondly, we proposed that Cybersecurity positively influences Uncertainty Avoidance, and thirdly, we suggested a significant positive effect of Uncertainty Avoidance on Digital Trust. The fourth proposed that Digital Trust is significantly related to Continual Usage of e-commerce platforms. All were confirmed at 95% confidence level, supporting our expectations (H1: $\beta = 0.272$, $p < 0.01$; H2: $\beta = 0.912$, $p < 0.001$; H3: $\beta = 0.689$, $p < 0.001$, H4: $\beta = 0.438$, $p < 0.001$). What this mean is that, Cybersecurity minimises uncertainty and encourages the people to trust or feel confident that they are safe to use e-commerce platforms, and leads them to continue using the platforms (Oguta, 2024). These are in line with existing studies (e.g., Sartono et al., 2024; Handoyo, 2024; Oguta, 2024). For instance, Oguta's (2024) study maintained that, security is a critical consideration in e-commerce due to the sensitive nature of online transactions. As such, smart businesses invest in Cybersecurity technologies to safeguard customer data and build trust (Handoyo, 2024). According to Hossain et al., (2024), trust minimises perceived risks associated with online shopping and makes customers comfortable enough to have repeated interactions and long-term engagement with the platform. Digital Trust is built by ensuring perceived reliability through Cyberseurity and consistent positive encounters or experiences of the platform's services (Hossain et al., 2024).

According to Blender and Felderer, (2023), cybercrime is escalating at an alarming rate, and nearly everyone has experienced some form of cyberattack (Stzelecki and Rizun, 2022). Consequently, users are feeling increasingly insecure and are therefore seeking clear signs of Cybersecurity before proceeding with online transactions, especially in cultures where Uncertainty Avoidance are very high (Ashraf et al., 2019; Crossler et al., 2018). Users seek convincing cues to trust or believe that the environment in which they are engaging in the e-commerce has appropriate safeguards or protection before they proceed (Vance et al., 2008; Oguta 2024).
Next, hypothesis 5, 6 and 7 were also highly significant (i.e., : H5: $\beta = 0.628$, $p < 0.001$; H6: $\beta = 0.114$, $p < 0.01$, H7: $\beta = 0.072$ $p < 0.01$). The significance of these hypotheses demonstrates that 1. the relationship between Cybersecurity and Digital Trust is mediated by Uncertainty Avoidance (H5). This indicate that, Uncertainty Avoidance helps to explain the effect of Cybersecurity on Digital Trust. Thus, Cybersecurity minimises the likelyhood of users avoiding engagement with e-commerce platforms as it allows people to trust that they are safe in using e-commerce platforms. While no study has established the mediation role of Uncertainty Avoidance in cyberspace, several studies have shown that, Uncertainty Avoidance moderates the relationship between Digital Trust and intention to adopt digital technology (e.g., Faqih 2022; Sartono et al., 2024).

Next, H6 demonstrates that ICT Skills mediates the relationship between Digital Trust and Continual Usage. ICT Skills are crucial for managing information security and effectively using e-commerce platforms (Thomas, 2018; Adams & Alhassan, 2021). They are the basic computer and internet skills used for operating, processing, and dissemination of information as well as changing, accessing and using software and hardware of computer and internet devices (Kusumaningtyas & Suwarta, 2015). The requisite ICT Skills equips users with the knowhow to be able to appreciate whether a particular Cybersecurity is genuine or effective, hence leading to Trust in the e-commerce platform at hand (Faqih, 2022). This is consistent with Valencia-Martinez et al. (2023) and Faqih (2022) which showed that, trust serves as a key indicator of perceived security and impacts on users' intention to continue engaging with an e-commerce platform. This is not to say that, with ICT Skills one cannot be defrauded, however, it puts one who has the skills at an advantage over one without the skills as they are more likely to detect and prevent cyberattack than one without the requisite skills (Ben-Asher & Gonzalez, 2015).

Lastly, H7 shows that, Cybersecurity significantly impacts on Continual Usage through the mediation of Uncertainty Avoidance, Digital Trust, and ICT Skills. This implies that Cybersecurity minimises users doubt or uncertainty and leads to Digital Trust which in turn impacts on ICT Skills and finally encourages users to continue patronising the platform. It suggests that, although consumers are seeking information systems security, they are skeptical of readily accepting any technology claiming to offer security (Rana & Chicone 2024). For instance, according to Rana and Chicone (2024), despite the benefits of Cybersecurity , a number of ethical concerns have been raised concerning their impact on privacy. Users seek trustworthy and convincing cues before embracing such technologies (Rana & Chicone 2024). The cues include ease of use, user friendly interface, quality systems, systems with high ethical standards and checks against cyber attacks (Vance et al., 2008; Han et al. 2023; Blender & Felderer 2023). Studies have established that people are more likely to trust and engage with e-commerce platforms

that implement robust security measures than those believed to have less robust security measure (e.g., Hossain et al., 2024).

Accordingly, the tech industry has created numerous security systems to mitigate risks or make attacks significantly more challenging (Blender & Felderer 2023). However, many people find these security technologies difficult to use (Sasse, 2005; Blender & Felderer 2023; Han et al., 2024). Their inability to easily navigate and use the technology irritates them and impacts on their trust in the technology (Johnson et al., 2008). This finding aligns with previous research that highlight the role of user competence in enhancing the effectiveness of security measures and trust in digital environments (Han et al., 2024; Blender & Felderer 2023).

CONCLUSION

In conclusion, the study successfully tested and confirmed seven hypotheses, demonstrating the critical role of Cybersecurity in fostering Continual Usage of e-commerce services and platforms. The findings underscores that, Cyberseurity not only directly influences an ongoing use of e-commerce platforms, but also plays a fundamental role in its affect of culture, in this case, by minimising doubt or uncertainty as a cultural trait, to build and sustain consumer Trust, which further enhances Continual Usage. This is consistent with prior literature, which highlights the importance of Cybersecurity in nurturing trust and loyalty in e-commerce contexts (Oguta 2024; Hossain et al., 2024; Sartono et al., 2024). Additionally, the study shows that ICT Skills significantly mediates the relationship between Trust and Continual Usage, reinforcing the idea that while users seek secure systems, they also require ease of use and user-friendly interfaces to maintain their trust and engagement with these platforms. The marginal impact of ICT Skills as a mediator between Cybersecurity and Continual Usage suggests that while technical competence is important, it may not be the sole factor in enhancing user trust and platform loyalty. Overall, the study underscores the necessity for e-commerce platforms to prioritize robust Cybersecurity, provide trustworthy cues including user-friendly interfaces and easy to use security measures to ensure sustained Digital Trust and Continual usage.

IMPLICATIONS

7.1 Theoretical implications

The theoretical implications of the study extends across multiple domains, particularly in the fields of information systems, e-commerce, and consumer behaviour. By confirming that Cybersecuriy significantly impacts Uncertainty Avoidance, Digital Trust and Continual Usage of e-commerce platforms, the study reinforces existing theories that emphasize the foundational role of security in digital environments. The study contributes to the broader understanding of how security measures are not just protective mechanisms but are integral to the user's decision-making process. This finding aligns with and expands upon the Social Exchange theory and Technology Acceptance Model (TAM) where Social Exchange theory sees trust as a result of a reciprocal process in which individuals trust institutions based on their previous experiences with their e-commerce platforms and their expectations of future benefits from their transactions (Park and Kim, 2023). The TAM suggests that perceived ease of use and usefulness are key factors influencing technology adoption. Here, Cybersecurity emerges as a critical component of perceived usefulness, directly affecting Uncertainty Avoidance, Digital Trust and Continual Usage of e-commerce platforms.

Additionally, the study's examination of Uncertainty Avoidance as a mediating factor between Cybersecurity and Digital Trust, as well as ICT Skills between Digital Trust and Continual Usage, adds a valuable layer of insight into the influence of culture and user competence on the development of Digital Trust. While prior research has acknowledged the importance of user competence (e.g. Vance et al., 2008; Blender and Felderer, 2023), this study highlights Culture and ICT Skills as significant facilitator of the relationship between Trust and the ongoing use of e-commerce services. This suggests that models of technology acceptance and usage must increasingly consider culture and user competence as variables that can promote the effectiveness of security measures in fostering trust.

The marginal effect of ICT Skills as a mediator between Cybersecurity and Continual Usage also invites further theoretical exploration. This finding could lead to a refinement of existing models, to provide more nuanced understanding of how user skills interact with security perceptions to influence trust and usage behaviours.

In conclusion, our findings provide a richer understanding of the dynamics that drive consumer behaviour in digital environments, offering a foundation for future research to explore the complex relationships between these variables.

7.2 Practical Implications

The study emphasized the significance of Cybersecurity , Uncertainty Avoidance, Digital Trust and ICT Skills effects on Continual Usage of e-commerce platforms in Ghana. This finding has practical implications for e-commerce businesses, policymakers, and individuals. In line with Parmer, (2024) and Maqableh et al. (2021) we recommend that e-commerce businesses must prioritize Cybersecurity to protect user data and ensure trust, investing in robust measures to safeguard against cyber threats. Moreover, Cybersecurity systems should be user-friendly to avoid frustrating users and eroding trust (Sasse, 2005; Chang and Chen, 2009). Providing clear and convincing cues of Cybersecurity , such as trust badges and secure payment gateways, can also enhance user trust. Additionally, e-commerce businesses can

offer training or support to enhance users' ICT Skills, which play a crucial role in mediating the relationship between Digital Trust and Continual Usage (Johnson et al., 2008). Regular security audits can help identify vulnerabilities and ensure the effectiveness of Cybersecurity measures. Policymakers can develop guidelines and regulations to ensure e-commerce businesses prioritize Information Security and protect user data. Educating consumers about the importance of Information Security and how to identify trustworthy cues can also help them make informed decisions when using e-commerce platforms. Ultimately, e-commerce businesses must continuously monitor user behaviour and adjust their Cybersecurity measures accordingly to ensure optimal trust and Continual Usage, maintaining a competitive edge in the market. Consumers should exercise caution before making purchases, as many shopping websites contain features that can trigger anxiety and attract criminals (Faqih, 2022; Hariharan et al., 2023). Moreover, it is crucial for consumers to improve their knowledge and ICT skills. Staying up-to-date with current security measures and becoming well-informed. Tech-savvy users are more likely to identify vulnerabilities in online platforms.

7.3 Limitations and directions for future research

This study has some limitations. First, it was conducted in Ghana, so future research should be carried out in other countries to provide a more comprehensive understanding of the impact of Cybersecurity on e-commerce across Africa. Secondly, the use of convenience sampling, along with the study's focus on a single country and a small sample size, limits the generalizability of the findings. We recommend using probability sampling across multiple countries to obtain more representative data for a broader perspective. Additionally, future studies could employ qualitative methods to explore people perceptions of security in e-commerce more deeply.

Declaration of interest statement:

This study is an original unpublished work that has not been submitted to any other journal for review. Its content has not been copyrighted, published previously, or under consideration for publication anywhere else.

Funding

This study was not funded by any grant from any funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

1. Adam, I. O., & Alhassan, M. D. (2021). Social Media and E-Commerce at the Global Level: Do ICT Access and ICT Skills Matter?. International Journal of E-Business Research (IJEBR), 17(4), 1-18.
2. Altuncu, Y., Aktepe, Ş. Ö., & İslamoğlu, G. (2012). Preliminary study for the development of Uncertainty Avoidance instrument in Turkey. Journal of Business Economics and Finance, 1(4), 34-48.
3. Alkhwaldi, A. F., Al-Qudah, A. A., Al-Hattami, H. M., Al-Okaily, M., Al-Adwan, A. S., & Abu-Salih, B. (2023). Uncertainty Avoidance and acceptance of the digital payment systems: a partial least squares-structural equation modeling (PLS-SEM) approach. Global Knowledge, Memory and Communication.
4. Alkhunaizan, A. S., & Ali, A. (2022). An analysis of increased usage of e-commerce during COVID-19. Indonesian Journal of Electrical Engineering and Computer Science, 25(2), 1123–1130. https://doi.org/10.11591/ijeecs.v25.i2.pp1123-1130
5. Altinay, L., & Taheri, B. (2019). Emerging themes and theories in the sharing economy: a critical note for hospitality and tourism. In International Journal of Contemporary Hospitality Management, 31(1), 180-193. https://doi.org/10.1108/IJCHM-02-2018-0171
6. Alzoubi, H. M., Alshurideh, M. T., Kurdi, B. Al, Alhyasat, K. M. K., & Ghazal, T. M. (2022). The effect of e-payment and online shopping on sales growth: Evidence from banking industry. International Journal of Data and Network Science, 6(4), 1369–1380. https://doi.org/10.5267/j.ijdns.2022.5.014
7. Amofah, D. O. (2022). Sustaining consumer E-Commerce adoption in Sub-Saharan Africa : Do trust and payment method matter? 1–20.
8. Ashraf, M., Ahmad, J., Sharif, W., Raza, A. A., Salman Shabbir, M., Abbas, M., & Thurasamy, R. (2020). The role of continuous trust in usage of online product recommendations. Online Information Review, 44(4), 745-766.
9. Azizah, S. N. (2021). Cyber-Crime and Fraud Victimization of Online Halal Meat Shops: A Negative Image Propagation. International Journal of Cyber Criminology, 15(1), 158–173. https://doi.org/10.5281/zenodo.4766540
10. Bazyl, L., Radkevych, O., Radkevych, V., & Orlov, V. (2020). Interdisciplinary approach to the economic-legal socialization of specialists in modern labor market. Utopia y Praxis Latinoamericana, 25(Extra 6), 208–218. https://doi.org/10.5281/zenodo.3987608
11. Barnard, L., & Wesson, J. (2004, October). A trust model for e-commerce in South Africa. In ACM International Conference Proceeding Series, 75(1), 23-32.
12. Bendler, D., & Felderer, M. (2023). Competency models for information security and Cybersecurity professionals: analysis of existing work and a new model. ACM Transactions on Computing Education, 23(2), 1-33.
13. Calder, B. J., Malthouse, E. C., & Schaedel, U. (2009). An experimental study of the relationship

between online engagement and advertising effectiveness. Journal of Interactive Marketing, 23(4), 321–331. https://doi.org/10.1016/j.intmar.2009.07.002

14. Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. Information & Management, 46(7), 411-417.
15. Chapman, A., Verdery, A. M., & Moody, J. (2022). Analytic Advances in Social Networks and Health in the Twenty-First Century. Journal of Health and Social Behaviour, 63(2), 191–209. https://doi.org/10.1177/00221465221086532
16. Darmiasih, M., & Setiawan, P. Y. (2020). Continual usage intention and its antecedents on using OVO e-wallet application in Denpasar. International Research Journal of Management, IT and Social Sciences, 8(1), 35–46. https://doi.org/10.21744/irjmis.v8n1.1104
17. Du, W., & Liang, R. Y. (2024). Teachers' Continued VR Technology Usage Intention: An application of the UTAUT2 Model. SAGE Open, 14(1), 21582440231220112.
18. Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. Computer Science & IT Research Journal, 5(3), 703-724.
19. Faqih, K. M. (2022). Internet shopping in the Covid-19 era: Investigating the role of perceived risk, anxiety, gender, culture, and trust in the consumers' purchasing behaviour from a developing country context. Technology in Society, 70, 101992.
20. Florea, N. V., Ionescu, C. A., Duică, M. C., Căpușneanu, S., Paschia, L., Stanescu, S. G., & Coman, M. D. (2022). Trends and Perspectives of Romanian E-Commerce Sector Based on Mathematical Simulation. Electronics (Switzerland), 11(15). https://doi.org/10.3390/electronics11152295
21. Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. In Source: Journal of Marketing Research (Vol. 18, Issue 1).
22. Fricker, R. D., & Schonlau, M. (2002). Advantages and disadvantages of Internet research surveys: Evidence from the literature. Field Methods, 14(4), 347-367.
23. Fuhse, J. A., & Gondal, N. (2022). Networks from culture: Mechanisms of tie-formation follow institutionalized rules in social fields. Social Networks. https://doi.org/10.1016/j.socnet.2021.12.005
24. Gangwar, S., & Narang, V. (2022). A survey on emerging cyber crimes and their impact worldwide. In Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 1583-1595). IGI Global.
25. Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? MIS quarterly, 981-1001.
26. Han, L., Ma, Y., Addo, P. C., Liao, M., & Fang, J. (2023). The role of platform quality on consumer purchase intention in the context of cross-border e-commerce: The evidence from Africa. Behavioural Sciences, 13(5), 385.
27. Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). Special issue on the use of Partial Least Squares (PLS) to address marketing management topics. Journal of Marketing Theory and Practice, 19(2), 139–151. https://doi.org/10.2753/MTP
28. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. In European Business Review (Vol. 31, Issue 1, pp. 2–24). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-11-2018-0203
29. Hajibabaee, F., Salisu, W. J., Akhlaghi, E., Farahani, M. A., Dehi, M. M. N., & Haghani, S. (2022). The relationship between moral sensitivity and caring behaviour among nurses in iran during COVID-19 pandemic. BMC Nursing, 21(1), 1–8. https://doi.org/10.1186/s12912-022-00834-0
30. Hariharan, J., Sheik, A. T., Maple, C., Beech, N., & Atmaca, U. I. (2023, June). Customers' perception of Cybersecurity risks in E-commerce websites. In International Conference on AI and the Digital Economy (CADE 2023). 53-60. 10.1049/icp.2023.2565
31. Hashim, S., Mohd Yasin, N., & Ya'kob, S. A. (2020). What constitutes student–university brand relationship? Malaysian students' perspective. Journal of Marketing for Higher Education, 30(2), 180–202. https://doi.org/10.1080/08841241.2020.1713278
32. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
33. He, Q., Li, Y., Wu, Z., & Su, J. (2022). Explicating the cognitive process of a physician's trust in patients: A Moderated Mediation Model. International Journal of Environmental Research and Public Health, 19(21). https://doi.org/10.3390/ijerph192114446
34. Hofstede, G. (1991). Cultures & organizations: Software of the Mind. Berkshire UK: McGraw-Hill.
35. Hofstede, G. (2001). Culture's consequences: Comparing values, behaviours, institution, and organizations accross nations (2nd edition). California: Sage Publications.
36. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis:

Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1-55.

37. Huo, T., Yuan, F., Huo, M., Shao, Y., Li, S., & Li, Z. (2023). Residents' participation in rural tourism and interpersonal trust in tourists: The mediating role of residents' perceptions of tourism impacts. Journal of Hospitality and Tourism Management, 54, 457–471. https://doi.org/10.1016/j.jhtm.2023.02.011
38. Interpol African Cyberthreat Assessment Report (2024) Outlook By the African Cybercrime Operations Desk - 3rd edition. https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf
39. Johnson, D. S., Bardhi, F., & Dunn, D. T. (2008). Understanding how technology paradoxes affect customer satisfaction with self-service technology: The role of performance ambiguity and trust in technology. Psychology & Marketing, 25(5), 416-443.
40. Kassim, E. S., Jailani, S. F. A. K., Hairuddin, H., & Zamzuri, N. H. (2012). Information system acceptance and user satisfaction: The mediating role of trust. Procedia-Social and Behavioural Sciences, 57, 412-418.
41. Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications, 9(1), 84-95.
42. Kinal, J. (2022). Peculiarities of e-commerce development: a case of Poland. Entrepreneurship and Sustainability Issues, 9(3), 50–63. https://doi.org/10.9770/jesi.2022.9.3(3)
43. Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Understanding the process of building institutional trust among digital payment users through national Cybersecurity commitment trustworthiness cues: a critical realist perspective. Information Technology & People.
44. Lauren, R. L, Shannon, G. T., & Maureen, L. A.(2021). Supplemental material for how a gratitude intervention influences workplace mistreatment: A Multiple Mediation Model. Journal of Applied Psychology. https://doi.org/10.1037/apl0000825.supp
45. Li, Y., Xu, Z., & Xu, F. (2018). Perceived control and purchase intention in online shopping: The mediating role of self-efficacy. Social Behaviour and Personality:An International Journal, 46(1), 99-105.
46. Liu, Z., Delaloye, M., Glassey Balet, N., Hersant, S., Gris, F., & Sciboz, L. (2022). Trust in the News: A Digital Labelling Solution for Journalistic Contents. Online Journal of Communication and Media Technologies, 12(2), e202207. https://doi.org/10.30935/ojcmt/11528
47. Löbbers, J., & Benlian, A. (2019). The effectiveness of IS certification in E-commerce: does personality matter? Journal of Decision Systems, 28(3), 233-259.
48. Ly, H. T. N., Khuong, N. V., & Son, T. H. (2022). Determinants Affect Mobile Wallet Continuous Usage in Covid 19 Pandemic: Evidence From Vietnam. Cogent Business and Management, 9(1). https://doi.org/10.1080/23311975.2022.2041792
49. Maqableh, M., Hmoud, H. Y., & Jaradat, M. (2021). Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction. Heliyon, 7(9).
50. Masuda, H., Han, S. H., & Lee, J. (2022). Impacts of influencer attributes on purchase intentions in social media influencer marketing: Mediating roles of characterizations. Technological Forecasting and Social Change, 174. https://doi.org/10.1016/j.techfore.2021.121246
51. Menon, D. (2022). Purchase and continuation intentions of over -the -top (OTT) video streaming platform subscriptions: a uses and gratification theory perspective. Telematics and Informatics Reports, 5, 100006. https://doi.org/10.1016/j.teler.2022.100006
52. Miao, M., Jalees, T., Zaman, S. I., Khan, S., Hanif, N., & Javed, M. K. (2021). The influence of e-customer satisfaction , e-trust and perceived value on consumer ' s repurchase intention in B2C e-commerce segment. 72172129. https://doi.org/10.1108/APJML-03-2021-0221
53. Mweshi, G. K., & Sakyi, K. (2020). Application of sampling methods for the research design. Archives of Business Research, 8(11), 180–193. https://doi.org/10.14738/abr.811.9042
54. Nassè, T. B. (2018). Religious practices and consumption behavior in an African context: An exploratory study on consumers in Burkina Faso. Ouagadougou, OR: Doctoral thesis, Aube Nouvelle University in cooperation with Cheikh Anta Diop University.
55. Naatu, F., Alon, I., & Uwamahoro, R. (2022). Micro-franchising in the bottom of the pyramid market: Rwanda. Journal of Social Entrepreneurship, 13(1), 71-91.
56. Naatu, F., Selormey, F. S., & Naatu, S. (2024). Determinants of digital technology adoption in sub-Sahara Africa: Ghana. International Journal of Emerging Markets, 1-23.
57. Nambisan, S., & Baron, R. A. (2007). Interactions in virtual customer environments: Implications for product support and customer relationship management. Journal of Interactive Marketing, 21(2), 42–62. https://doi.org/10.1002/dir.20077

58. Ogar, J. O. (2022). Degree Mills and the Question of Educational Quality. November.
59. Palmié, M., Miehé, L., Oghazi, P., Parida, V., & Wincent, J. (2022). The evolution of the digital service ecosystem and digital business model innovation in retail: The emergence of meta-ecosystems and the value of physical interactions. Technological Forecasting and Social Change, 177(January). https://doi.org/10.1016/j.techfore.2022.121496
60. Park, J. Y., & Kim, C. (2023). The role of organizational justice and social interaction in mitigating the negative effects of high-performance member retailers on strategic integration. Journal of Retailing and Consumer Services, 72. https://doi.org/10.1016/j.jretconser.2022.103238
61. Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. Journal of operations management, 30(6), 467-480.
62. Pieters, W. (2011). Explanation and trust: what to tell the user in security and AI?. Ethics and information technology, 13, 53-64.
63. Pinem, A. A., Immanuella, I. M., Hidayanto, A. N., & Phusavat, K. (2018). Trust and its impact towards continuance of use in government-to-business online service. Transforming Government: People, Process and Policy, 12(3/4), 265-285.
64. Pomeroy, J. (2020). The booming digital economy. HSBC Global Research, 1-41. https://www.research.hsbc.com/R/34/scLRsql
65. Rahmayanti, P. L. D., Dharmanegara, I. B. A., Yasa, N. N. K., Sukaatmadja, I. P. G., Pramudana, K. A. S., Rahanata, G. B., Giantari, I. G. A. K., & Martaleni. (2022). What drives millennials and zillennials continuously using instant messaging? Perspective from indonesia. International Journal of Data and Network Science, 6(1), 17–26. https://doi.org/10.5267/J.IJDNS.2021.11.001
66. Rajaonah, B. (2017). A view of trust and information system security under the perspective of critical infrastructure protection. Revue des Sciences et Technologies de l'Information-Série ISI: Ingénierie des Systèmes d'Information, 22(1), 109.
67. Rana, S., & Chicone, R. (2024). Navigating the paradox of AI in Cybersecurity : unpacking societal optimism and ethical skepticism. Issues in Information Systems, 25(1), 175-187.
68. Rezaei, M., & Bresciani, S. (2020). What drives the process of knowledge management in a cross-cultural setting. 32(3), 485–511. https://doi.org/10.1108/EBR-06-2019-0127
69. Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. Applied Sciences, 13(2), 1020.
70. Sartono, Y., Astuti, E. S., Wilopo, W., & Noerman, T. (2024). Sustainable Digital Transformation: Its Impact on Perceived Value and Adoption Intention of Industry 4.0 in Moderating Effects of Uncertainty Avoidance. F1000Research, 13(821), 1-28.
71. Sasse, M. A. (2005). Usability and trust in information systems. Edward Elgar.
72. Saputra, R. A., Amrullah, R., Triono, A., & Refsi, B. (2022). Management of Improvement of Cyber Crime at the Time of the COVID-19 Pandemic Happening Restorative Justice. Scholars International Journal of Law, Crime and Justice, 5(7), 286–293. https://doi.org/10.36348/sijlcj.2022.v05i07.006
73. Shakeri, S., Veen, L., & Grosso, P. (2022). Multi-domain network infrastructure based on P4 programmable devices for Digital Data Marketplaces. Cluster Computing, 25(4), 2953–2966. https://doi.org/10.1007/s10586-021-03501-2
74. Shin, D. (2021). International Journal of Human - Computer Studies The effects of explainability and causability on perception , trust , and acceptance : Implications for explainable AI. 146(October 2020).
75. Shiroka-Pula, J., Bartlett, W., & Krasniqi, B. A. (2023). Can the Government Make Us Happier? Institutional Quality and Subjective Well-Being Across Europe: A Multilevel Analysis Using Eurobarometer Survey 2019. Applied Research in Quality of Life, 18(2), 677–696. https://doi.org/10.1007/s11482-022-10099-z
76. Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. Information Systems and E-Business Management, 20(1), 57–78. https://doi.org/10.1007/s10257-021-00545-0
77. Strzelecki, A., & Rizun, M. (2022). Consumers' change in trust and security after a personal data breach in online shopping. Sustainability, 14(10), 5866.
78. Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management, 12(3), 1-23.
79. Thomas, A., & Gupta, V. (2021). Social Capital Theory, Social Exchange Theory, Social Cognitive Theory, Financial Literacy, and the Role of Knowledge Sharing as a Moderator in Enhancing Financial Well-Being: From Bibliometric Analysis to a Conceptual Framework

Model. Frontiers in Psychology, 12. https://doi.org/10.3389/fpsyg.2021.664638

80. Thurik, A. R., Audretsch, D. B., Block, J. H., Burke, A., Carree, M. A., Dejardin, M., Rietveld, C. A., Sanders, M., Stephan, U., & Wiklund, J. (2023). The impact of entrepreneurship research on other academic fields. Small Business Economics. https://doi.org/10.1007/s11187-023-00781-3
81. Tofan, M., & Bostan, I. (2022). Some Implications of the Development of E-Commerce on EU Tax Regulations. In Laws (Vol. 11, Issue 1). MDPI. https://doi.org/10.3390/laws11010013
82. Trabucchi, D., Patrucco, A. S., Buganza, T., & Marzi, G. (2023). Is transparency the new green? How business model transparency influences digital service adoption. Technovation, 126. https://doi.org/10.1016/j.technovation.2023.102803
83. Ullah, N., Al-Rahmi, W. M., Alzahrani, A. I., Alfarraj, O., & Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments. Sustainability (Switzerland), 13(4), 1–18. https://doi.org/10.3390/su13041801
84. Valencia-Martinez, C. A., Gaona-García, P. A., & Montenegro-Marin, C. E. (2023). Design of a trust system for e-commerce platforms based on quality dimensions for linked open datasets. Journal of Information Systems Engineering and Management, 8(1).
85. Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: the effects of system quality and culture. Journal of management information systems, 24(4), 73-100.
86. Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly, 157-178.
87. Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. Journal of the Academy of Marketing Science, 44(1), 119–134. https://doi.org/10.1007/s11747-015-0455-4
88. Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. Journal of King Saud University-Computer and Information Sciences, 36(4), 102031.
89. Wang, C., Zhou, R., & Lee, M. K. (2021). Can loyalty be pursued and achieved? An extended RFD model to understand and predict user loyalty to mobile apps. Journal of the Association for Information Science and Technology, 72(7), 824-838.
90. Wu, C., Huang, S., & Yuan, Q. (2022). Seven important theories in information system empirical research: A systematic review and future directions. In Data and Information Management (Vol. 6, Issue 1). Elsevier Ltd. https://doi.org/10.1016/j.dim.2022.100006
91. Xu, L., Wang, J., & Xu, D. (2022). Integrating individual factors to construct recognition models of consumer fraud victimization.

Appendix 1. Factor Measurement Items and Source

Variables	Measurement Items	Source
Information Security	1. I have ever been a victim of e-commerce service fraud. 2. E-commerce service platforms manage my personal information well 3. Third parties can easily access my basic credentials on the e-commerce platforms I use. 4. I receive messages from unauthorised sources because of my usage of e-commerce platforms? 5. E-commerce service platforms give me updates on security issues when necessary?	Adapted from Calder et al., (2009)
Individual Trust	1. I feel confident when using e-commerce service platforms 2. Ecommerce service platforms are consistent in service delivery that is why I rely on them a lot? 3. Ecommerce service providers have a positive relationship with customers that is why use their platforms	Adapted from Nambisan and Baron, (2007)

	4. Ecommerce service providers are experts in their services and so it is easy to trust them 5. My privacy is assured when using e-commerce service platforms	
ICT Skills	1. I have knowledge in the use of ICTs for e-commerce 2. I can use computers for online activities 3. I don't own a smartphone, laptop, or computer, but I still use e-commerce service platforms] 4. I am skilful in web navigation] 5. I can use computers to conduct transactions electronically	Adapted from Nambisan and Baron, (2007)
Uncertainty Avoidance	1. I feel stressed when faced with situations for which the results cannot be predicted	Altuncu, Aktepe and İslamoğlu, (2012)
	2. I get worried when the end results of a technology is not known	
	3. I am not open to new learning	
	4. I like to have control over my future	
	5. I do not like to choose risky alternatives when making decision	
Continual Usage	1. I use e-commerce services regularly 2. I will continue using e-commerce services than I use any alternative means (e.g., physical shops)] 3. I will continue using e-commerce services rather than discontinue their use 4. It is worth using e-commerce service platforms when they are available 5. Ecommerce service platforms are fast, convenient and easy to use that is why I use them	Rezaei and Bresciani, 2020

(Source: Authors' Construct, 2023)