Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Master's Thesis

USER PERCEPTIONS AND BEHAVIORAL INTENTIONS TOWARDS PRIVACY AND SECURITY ONLINE

DEBORAH ASIABA JOHNSON

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Deborah Asiaba Johnson

Economics and Management

Thesis title

Users' perceptions and behavioral intentions towards privacy and security online

---

Objectives of thesis

The main objective of the thesis is to build and test a model of users' perceptions and behavioral intentions towards privacy and security online.

Partial objectives:
1. To review existing models of privacy and security online.
2. To prepare and conduct a survey among users.
3. To conduct statistical analysis, evaluate results and interpret findings.

Methodology

The theoretical part of the work is based on the study and analysis of professional and scientific information sources. The thesis focuses on user perceptions and behavioral intentions toward privacy and security online with a specific focus. The researcher will employ the mixed-method approach based on the study's objectives. On this basis, both qualitative and quantitative data will be used. By synthesizing knowledge of the theoretical part and evaluating the results of the practical part, the conclusions of the work will be formulated.

The proposed extent of the thesis

80 pages

Keywords

Online Risk, User Perception, Online Experience, User Trust, Behavioral Intentions

---

Recommended information sources

Gupta, M.P. and Dubey, A., 2016. E-commerce-study of privacy, trust and security from consumer's perspective. transactions, 37, p.38.

Hammouri, Q., Majali, T., Almajali, D., Aloqool, A. and AlGasawneh, J.A., 2021. Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review. Annals of the Romanian Society for Cell Biology, 25(6), pp.17083-17093.

Hariguna, T. and Berlilana, B., 2017. Understanding of antecedents to achieve customer trust and customer intention to purchase e-commerce in social media, an empirical assessment. International Journal of Electrical and Computer Engineering, 7(3), p.1240.

Javaria, K., Masood, O. and Garcia, F., 2020. Strategies to manage the risks faced by consumers in developing e-commerce. Insights into Regional Development, 2(4), pp.774-783.

Mahliza, F., 2020. Consumer trust in online purchase decision. EPRA International Journal of Multidisciplinary Research (IJMR), 6(2), pp.142-149.

Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. Indonesian Journal of Electrical Engineering and Computer Science, 21(2), 1065-1072.

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 2. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 21. 12. 2022

Declaration

I declare that I have worked on my master's thesis titled “User perceptions and behavioural intentions towards privacy and security online” by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 31.03.2023 _____

Deborah Asiaba JOHNSON

Acknowledgement

I would like to thank God Almighty, my supervisor Ing. Miloš Ulman, Ph.D. and my friends and families for their support and advice during my work on this thesis.

User perceptions and behavioural intentions towards privacy and security online.

Abstract

The study's primary goal was to examine the right models that illustrate the factors that influence online privacy and security. The study employed the explanatory research method to examine how different variables affected internet privacy and security. From the literature review, three models were inferred. The interaction between cultural, institutional, demographic, and perceived privacy risk on online privacy and security was the subject of the first existent model. The outcome revealed an 88.9% coefficient of determination. This means that 88.9% of the differences in online privacy and security may be accounted for by the factors. Model One has the greatest adjusted R-square by chance. The second model included relationships between the inherent features of the consumer, situational circumstances, website characteristics, the interaction between the client and the website, and laws and government privacy protection about online privacy and security. The modified R-square for model two was 55.5 percent. The third and final model included elements like established connections on privacy and security online, control over information and how it was used, and short-term transactions. The modified R-square for this was 50.1 percent. The study's main finding is that cultural, institutional, demographic, and perceived privacy risk variables influence what privacy and security approach is best for online learning clients.

Keywords: Online Risk, User perception, Online Experience, User Trust, Behavioural Intentions, Ghana, Online Transactions, Security, Payments, Online Shopping

Vnímání uživatelů a záměry chování vůči soukromí a bezpečnosti online.

Abstrakt

Primárním cílem studie bylo prozkoumat správné modely, které ilustrují faktory, které ovlivňují soukromí a bezpečnost online. Studie použila vysvětlující výzkumnou metodu k prozkoumání toho, jak různé proměnné ovlivnily soukromí a bezpečnost internetu. Z přehledu literatury byly odvozeny tři modely. Interakce mezi kulturním, institucionálním, demografickým a vnímaným rizikem soukromí v oblasti soukromí a bezpečnosti online byla předmětem prvního existujícího modelu. Výsledek odhalil 88,9% koeficient stanovení. To znamená, že 88,9% rozdílů v soukromí a zabezpečení online může být způsobeno faktory. Model One má největší upravený R-čtverec náhodou. Druhý model zahrnoval vztahy mezi inherentními rysy spotřebitele, situačními okolnostmi, charakteristikami webových stránek, interakcí mezi klientem a webem a zákony a vládní ochranou soukromí týkající se soukromí a bezpečnosti online. Upravený čtverec R pro model dva činil 55,5 procenta. Třetí a poslední model zahrnoval prvky, jako jsou navázaná připojení k soukromí a zabezpečení online, kontrola nad informacemi a jejich používáním a krátkodobé transakce. Upravený R-čtverec pro to byl 50,1 procenta. Hlavním zjištěním studie je, že kulturní, institucionální, demografické a vnímané proměnné rizika soukromí ovlivňují, jaký přístup k ochraně soukromí a zabezpečení je nejlepší pro klienty online učení.

Klíčová slova: Riziko Online, vnímání uživatelů, online zkušenost, důvěra uživatelů, záměry chování, Ghana, online transakce, bezpečnost, platby, online nakupování

Table of Content

Introduction

As result of the tremendous increase in Internet users over the past ten years, online privacy has become one of the most serious issues in the networked society and online business. According to a poll, 94% of US consumers think that internet privacy is important (Lili & Min, 2021). Internet users in the US report feeling "very" or "extremely" concerned about their online privacy, and 88% of them think it is unjust when companies track customers without their permission (Story et al, 2021).

Ghanaians who purchase online and use the Internet (97.9%) think that securing personal information is very essential or important. 86.6% of the time, Ghanaian internet users worry about their personal information being taken (Baako, Umar & Gidisu, 2019). In Ghana, 85% of Internet users say they worry "somewhat or severely" about privacy. In addition, the Internet economy is now a bigger part of the world economy. The high level of privacy concerns among Internet users is a hindrance to the expansion of the online economy. Additionally, privacy issues have become a prominent focus of discussion with the development of modern technologies such as smart phones and cloud computing. Nonetheless, a lot of global firms need to pay particular attention to privacy concerns in various countries.

Businesses would suffer major repercussions if privacy issues are not appropriately managed. Understanding the numerous privacy issues that Internet users in Ghana have been vital for organizations who want to conduct business in both countries. Despite yet, there are cultural differences among the Ghanaian nations. The impact of various cultural elements and other demographic factors on privacy issues in Ghana must be investigated. There are other factors that impact online trading privacy in addition to these worries. This study employs consumers who make purchases through Ghanaian trading platforms to analyse other models to better understand the factors that affect online privacy and security.

Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to build and test a model of user's perceptions and behavioural intentions towards privacy and security online.

The partial objectives of the study are to:

- To review existing models of privacy and security online
- To prepare and conduct a survey among users.
- To conduct statistical analysis, evaluate results and interpret findings.

2.2 Methodology

The "study's focus will be on those who do online transactions in Ghana using payment methods such credit cards on websites like Jumia, Jiji, Tonaton, KiKUU, Telefonika, and Maxbuy Online shopping platforms.

Figure 1: Map of Ghana

Source: Ghana Permanent Mission to the United Nations (2021)

The examination and analysis of authoritative and scholarly information sources provide the foundation of the theoretical portion of the task. The thesis has a unique emphasis on user perceptions and behavioural intentions about internet privacy and security. The mixed-method technique will be used by the researcher depending on the goals of the investigation. Based on this both qualitative and quantitative data will be used. The conclusions of the work will be created by combining theoretical knowledge and assessing the outcomes of the practical component.

Literature Review

3.1 Theories in Technology Adoption

3.1.1 Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA) was founded in 1975 by Fishbein and Ajzen with the goal of predicting and explaining individuals' volitional conduct and understanding its psychological underpinnings. According to the idea, for humans to be rational in nature, they must behave based on the knowledge available, with a set of behavioural intents that serve as the primary determinants of their rational behaviours (Fidelis, 2017). According to the idea, intentions are the most important predictor of an individual's conduct, and any external impact on behaviour will be through their intentions. As a result, "Intention" refers to the motive that drives an individual's intended activity. Additionally, Fishbein and Ajzen (2015) claimed that personal (intention) and societal influence are two significant factors of intents.

The model develops the attitude, social influence, and intention variables that are used to predict behaviour. TRA hypothesizes that an individual's behavioural intention (BI) to do a behaviour is simultaneously governed by the individual's attitude toward completing the action (ATB) and subjective norm (SN), which together comprise an individual's overall assessment of what is relevant or otherwise. Individuals' positive or negative sentiments about executing the goal activity were described as their attitude (Fishbein & Ajzen, 2015).

This idea, however, has major flaws, which are outlined below: First and foremost, the idea implies that humans are sensible enough to act on the knowledge they have. Yet, this is too harsh, given people have been shown to be illogical in certain behaviours and under specific circumstances. People may possess unreasonable and diverse ideas that influence their decisions at some point. According to Montano and Kasprzyk (2018), the theory of reasoned action is successful in describing behaviour when volitional control is strong, but it fails to explain behaviour when volitional control is low. According to Fishbein and Ajzen, to

anticipate an individual's conduct, attitude and purpose must be contextually and temporally related. Moreover, Yousafzai et al. (2018) stated that the theory can only be applied to volitional activity, which means that the behaviour must have been planned before the act.

Additionally, there is a high danger of conflating attitudes and norms since attitudes are frequently reframed as norms and vice versa (Samaradiwakara & Gunawardena). Because of these flaws, the Theory of Planned Behaviour was developed in attempt to increase knowledge of the acceptance theories. This model was expanded to account for changes in the variables, and the final model was dubbed "Theory of Planned Behaviour." Several nations are rapidly embracing technological innovations, notably in online shopping, to improve in technology and its applications. Again, owing to the competitive nature of global business combined with consumer satisfaction, many firms are turning to online platforms to conduct business with their suppliers, present and prospective customers (Acquah, 2016). Nonetheless, there are still certain critical challenges concerning the usage of information technology and its security. With relation to risk management, the information technology risk management concept is viewed as a system of a larger company. Before now, security breaches in the company's information systems occurred at the network level. These days, e-commerce web application vulnerabilities are a constant source of assaults from both internal and external sources for the purpose of fraud and identity theft. The use of EC has increased dramatically in recent years. According to Eurostat, EC penetration increased 150% between 2021 and 2021.

This increase was unique to the EU. Notwithstanding this rise, the proportion of customers making online transactions remains low across most of Europe. In 2021, just 38% of European Union customers completed online purchases in the previous three months, while only 14% of enterprises' income came from the EC. By researching this trend, we noticed that privacy concerns about personal information were the second-most common reason for clients in the European Union not adopting EC, trailing only security concerns. Individuals' confidential data

privacy is a fundamental topic that has been extensively addressed in marketing writing, both offline (Jones, 1991) and online. Yet, because privacy issues have been included in online commerce models that are fundamentally based on trust, the research has downplayed their importance in the EC context. or depending on the estimated amount of risk Furthermore, most of the previous research has focused on how privacy concerns impact customers' intentions to buy online or whether they really do buy online. Brown and Muchira (2021). As a result, the theoretical framework provided by these studies is insufficient to account because privacy concerns influence critical variables of consumer behaviour prior to making a pre-buy or purchase choice. The information supplied by this study fills this void. Understanding in depth consumers' online information privacy issues is critical for maximizing EC's potential. Despite a few ground-breaking works, such as Miyazaki and Fernandez's (2018) and Sheehan and Hoy's (2018), no studies have offered a clear theoretical framework to Internet privacy challenges. Malhotra, Kim, and Agarwal's (2021) work are important for providing a conceptual framework and establishing a specific scale for online privacy problems. The authors claim that there are three major parts to the privacy concerns of Internet users: collection, control, and knowledge.

In this sense, "collection" refers to a person's concern about the amount of personal data controlled by others in comparison to the benefits achieved. The degree of control over data reflects consumers' ability to exercise choice over the acquisition, use, and disposal of their personal information. Finally, one's degree of awareness is reflected in how well informed they are on the company's privacy practices. Numerous consumer behaviour studies, including studies centred on the technology acceptance model and the theory of planned behaviour (TPB), have addressed the issue of online privacy, illustrating the topic's popular interest. Multiple studies (for example, Van Slyke, Shim, Johnson, and Jiang) have shown that individuals' level of privacy concern is correlated with their level of risk perception (2016) and

also has a detrimental effect on trust (e.g. Eastlick et al., 2016; Liu, Marchewka, Lu, & Yu, 2015; Van Dyke, Midha, & Nemati, 2017), intention to buy online (e.g. Liao, Liu, & Chen, 2020 Despite its popularity and success, the TPB has not been without criticism. One sort of criticism concerns the theory's sufficiency—the idea that attitudes, subjective standards, and perceptions of behavioural control are enough to predict intentions and conduct.

3.1.2 Theory of Planned Behaviour (TPB)

When considering the predictability of the TRA across studies, one of its intrinsic flaws is that if the conduct under research is not fully voluntary, another issue becomes predictable. To begin, one must be able to distinguish between behaviours and intentions. This might be problematic since, in addition to one's goals, a range of circumstances influence how one's conduct manifests. Second, the model makes no provision for determining whether the chance of failing to perform is related to one's conduct or one's goals. To address these issues, Ajzen (1985) expanded the theory of reasoned action in 1991 by incorporating a new concept termed perceived behavioural control, which predicted behavioural intents and conduct. The degree of control individuals feel they have over executed an activity was termed as perceived behavioural control. According to this theory, two major elements impact human conduct: (1) attitude toward behaviour and (2) the influence of social environment and general subjective standards on behaviour. The study discovered that direct connections from attitude to actual conduct and from subjective norm to attitude can increase the model's predictive ability and explanatory content. This theory so explains why cultural variables, demographic factors, institutional factors, and perceived dangers impact individual behaviour in their online interactions. When respondents are influenced by environmental and institutional circumstances, their behaviour changes. Moreover, website encounters might impact an individual's online security and privacy thinking and approach.

3.1.3 Technology Acceptance Model (TAM) and Its Extensions

The Technology Acceptance Model (TAM) by Davis et al. (1989) which is a modification of the Theory of Reasoned Action (TRA), was adapted to inculcate the modelling of users' adoption of Information Systems in the workplace. TAM posits that views regarding utility and ease of use are the major drivers of information technology adoption, whereas the TRA argued that beliefs impact attitude. The goal is to describe the impact of user perceptions of the system, its qualities, influence, and acceptability. In an ideal world, a model would be useful not just for prediction but also for explanation, allowing academics and practitioners to determine why a specific system may be undesirable and take necessary remedial actions. TAM's primary goal is to create a foundation for tracking the effect of external circumstances on internal beliefs, attitudes, and intentions.

Many objections have been levelled towards the TPB. Is it sufficient to establish a theory of all volitional behaviour on only four explanatory ideas? This subject mentions an intriguing trade-off between parsimony and validity. For example, the idea has been criticized for minimizing the function of emotions and emphasizing the necessity of conscious cognition in determining the amount of predicted emotional impacts (Sheeran, Gollwitzer, & Bargh, 2021). 2021) (Conner, Gaston, Sheeran, & Germain). Additionally, the TPB's static explaining approach makes it difficult to understand the established effects of behaviour on thoughts and behaviours (McEachan et al., 2020; Sutton, 1994).

Several people question if the model's hypotheses can be disproven by experiments or if they are just common-sense claims (Ogden, 2017; Smedslund, 1978). Moreover, it looks strange and would put doubt on the data rather than the underlying theory if findings under control settings revealed that people were more likely to engage in behaviours they disliked, felt incapable of, or did not want to engage in. Despite finding that authors of studies with results that contradict TPB expectations (for instance, null correlations amongst variables

hypothesized to be extremely correlated) not often question the theory's validity, Ogden (2017) discovered that authors of such studies instead consider alternative explanations, such as the operationalization of their study measures. When it comes to predicting when a credit union employee will begin using the internet, the UTAUT model outperforms the TAM. This conclusion is supported by the discriminant analysis classification result, which shows an increase from 71.0 to 81.5 percent. The most discriminating UTAUT elements are internet anxiety and self-efficacy, while the most discriminatory TAM variables are ease of use and staff creativity. Perceptions of the internet, notably online anxiety, internet-self efficacy, and personal innovativeness, play an important impact in the decision to join the internet.

3.2 The Concept of E-commerce

The word "e-commerce" is extremely wide, however a definition is provided with the study context. A historical summary is offered at the start. The Internet is the foundation of e-commerce. The Internet's beginnings may be traced back to the 1960s, far before the advent of contemporary e-commerce. APRANET, the Internet's forerunner, was founded as a research network connecting just a few research institutions in the United States. Andrews et al., 2021). Commercial usage of the Internet was not permitted until the early 1990s. As a result, it is widely recognized that the emergence of e-services began around that time. Dell, Cisco, and Amazon were among the first significant business entities to take advantage of the Internet's capabilities. But, a few years later, numerous corporate organizations were striving to conduct commercial transactions over the Internet, lead to in a rise in e-commerce. The initial wave of E-commerce was a "pamphlet" with static homepages. This performed the fundamental job of distributing material and contacts to clients. The second wave of E-commerce was capable of handling electronic transactions, such as buy and sell operations, through the Internet. It was a significant milestone because there were several concerns with payment security. PAYPAL was the first firm to offer a secure payment mechanism (Grabianowski and Crawford, 2015).

The third “wave of E-commerce was intended to interact with commercial societies, consumers, producers, and other investors in real-time used in information sharing and exchange (Fingar, 2018). E-commerce encompasses any type of electronic economic activity, such as Online services, or simply the sheer availability of web content with the potential to lead to transactions via fax machines and phone (Coffee, 1998; Riggins and Rhee, 1998; Riggins, 1998). This view of e-commerce is extremely archaic. Supporters of industry organizations and economic efficiency theory argue that E-commerce may lower transaction and search costs (Kalakota and Whinston, 1997; Tapscott, 2018; Janssen and Sol, 2018). It will hasten the movement of power toward customers, resulting in perfect competition and, as a result, lower overall profitability for enterprises and the industry (Slywotzky, 2020; Porter, 2020). Nowadays, e-commerce is seen as a critical component of corporate growth. This covers the use of Fintech, with its many ecommerce models and operations.

3.2.1 Classification of E-commerce Models

Rayport and Jaworski, 2020; Kinder, 2020 outlines seven types of business models that use e-commerce (see Table 2). In most marketplaces, the major models are business-to-business and business-to-customer. Customer to Customer and Customer to Business models are centred on the consumer. Customer-to-Business refers to situations in which individuals establish buyer groups to obtain better deals from online providers, such as online courses and trip tickets. Customer-to-Customer refers to a community created to pursue unique interests in which individuals exchange ideas, services, and products. For example, tori.fi and many topic-specific forums. The final three categories include government interactions with corporations, other authorities, and consumers.

Some academics, however, classify Business-to-Government as Business-to-Business. A business contractor is affiliated with the government. This research assumes this and lumps B2G under the B2B group.

Table 2. Classifications of E-Commerce Models. (Rayport and Jaworski, 2020; Kinder, 2020)

B2B – Business-to-Business	Estimated about 75% of E- commerce
B2C – Business-to-Consumer	For home shopping, banking, on-line brokerage, travel.
C2B - Customer-to-Business	C2B refers to a group of individuals forming as a buyer group to transact activities with businesses,
C2C - Consumer-to-Consumer	On-line community for research, sales, or any other exchange, e.g., tori.fi
B2G – Business-to- Government	Tendering via E-commerce, Customs declaration
G2G – Government-to- Government	Electronic Government, On-line school, Global ICT planning and implementation
G2C – Government-to- Consumer	Electronic votes, Travel information Kiosk, Electronic licenses renewal

This study concentrates on the first two business-to-business and business-to-consumer models. This is because these two models have the maximum effect on businesses and, as a result, global markets.

3.3 Online Privacy

Online privacy refers to the act of selective disclosure (of oneself) in an online setting. Online privacy is typically characterized as Internet users' concern about (1) their control over information acquired during online activity and (2) control over the use of information gained during online activity (Barakovic, Kurtovic, Bozanovic, Mirojevic, Ljevakovic, Jokic & Husic, 2016).

As a result, online privacy addresses users' concerns about: (1) the level of control users have over the obtained information, (2) the quantity and quality of information collected about them by a specific website, and (3) users' knowledge of privacy practices (Symantec Norton Department, 2012). Several factors influence this privacy management process, including individual characteristics, geographical distances and impediments, and a variety of societal contexts. The section that follows provides an overview of the components that could affect Internet users' privacy issues.

3.3.1 Factors that influence Internet users' privacy concerns – User Perception

Sheehan and Hoy conducted one of the first studies on customers' concerns about their internet privacy (2011). The authors identified three factors that influence customers' concerns about their online privacy: (1) Established relationship, which resolves issues regarding the existence of ties between a client and a website, as well as past contact between the two. (2) Control over the gathering and use of information. (3) Short-term transaction, which relates to transaction exchange difficulties including the type of information being traded for a specific advantage. One of the models for the analysis includes the factors.

3.3.1.1 Established relationship

Experience on the website would enhance the relationship the user has with the interface. The established relationship might create trust on the website where customers and users would upload their sensitive information without fear and panic. The established relationship therefore influences the internet privacy concerns. According to theory of reasoned behavior, an existing relationship would create a form of consistency in dealing with the website.

3.3.1.2 Control over information collection and usage of information

The control that customer and users have in the information they collect, and use has a positive and considerable influence on the internet privacy. Controlling information will also make users selective on the details they need to gather on the internet and the kind of information

they need to use. Having these control would also prevent them from sharing information that are sensitive and as well as using sensitive information from the internet.

3.3.1.3 Short term transaction

Short-Term Purchases – Securities acquired with the expectation of selling them within a brief period, often less than one year, to capitalize on the securities' short-term price changes. Because to the brief duration of the transaction, users and consumers may not have enough time to verify the legitimacy of the website. This might jeopardize their privacy.

The next model also used the study by Barakovic et al. (2016) as basis for the factors affecting privacy concerns. The model included 1. Customer and website relationship, 2. Web site characteristics, 3. Situation factors, 4. customer-intrinsic characteristics and 5. Legislation and government privacy protection.

3.3.1.4 Customer-intrinsic characteristics

Different people react differently to the same or comparable events. As a result, it is essential to consider individual traits while talking about privacy perception. Numerous academics have investigated how different personal traits affect worries about internet privacy. For instance, men are more inclined than women to secure their internet information (Milne, Rohm, & Bahl, 2004). Additionally, accessing the Internet for extended periods of time reduces worries about online privacy (Skippari, Kajalo & Lindblom, 2022). People who have had their privacy violated in the past are more concerned about privacy protection. Additionally, with their current online engagement, they are more circumspect about sharing their personal information (Dolnicar & Jordaan, 2006).

3.3.1.5 Situation Factors

Context considerations refer to the idea that an individual might behave differently in the same event but under different circumstances. These circumstance characteristics are often individual and represent the current attitude and demands, as well as previous experience in a

certain situation. The type and quantity of information sought in an online transaction is commonly referred to as situational variables that impact Internet users' privacy perception. Castaeda and Montoro (2007) define information sensitivity as individuals' privacy concerns about a specific sort of information in each scenario.

3.3.1.6 Web site characteristics

Internet users' opinions of a given website is influenced by both their present interactions and their assessments of earlier encounters. This assessment often has something to do with how people feel about an e-service website. Therefore, issues pertaining to the website features cannot be ignored while considering consumers' perceptions of online privacy. A strong brand reputation not only reduces customers' privacy worries but also favorably affects their confidence in an e-tailer. According to Metzger (2006), users can estimate an e-behavior tailers in their upcoming connections by looking at their reputation. When deciding whether to provide the required personal information, the combined impact of Internet trust and personal Internet interest can take precedence over privacy concerns, even though privacy concerns have a detrimental impact on e-commerce usage (Dinev & Hart, 2006). Websites provide new chances to create and maintain client interactions, but they also indicate a tension between two tendencies (Geissler, 2001). (Dinev & Hart, 2004). The first trend may be summed up as the necessity to collect and use a lot of consumer personal data to provide better customer service. The second trend is the escalating dangers to customer privacy.

3.3.1.7 Customer and web site relationship

Individuals' perceptions and attitudes toward information gathering (done by a specific web site) during online activity are typically tied to the customer and web site relationship group of characteristics. The foundation for privacy protection, known as fair information practices (FIPs), is now included into several national legislation. According to Bhasin (2006), FIPs are governed by five principles: notification, choice, access, integrity and security, and

enforcement. Control and understanding of privacy practices are two new characteristics of information privacy that the Internet Users' Information Privacy Concerns scale (IUIPC) (Malhotra, Kim, & Agarwal, 2004) presents. Control is the term used to tell how much power individuals have over the personal data that has been gathered. Individuals must comprehend and be familiar with the techniques used to alter personal information to be aware of privacy practices.

3.3.1.8 Legislation and government privacy protection.

Customers' perceptions of how the government and laws safeguard their online privacy are among the elements included in the legislation and government protection group. The impression and knowledge of government protection among consumers enhances their trust in online transactions, which in turn boosts e-commerce adoption (Ashworth & Free, 2006). Internet users think that huge businesses and governmental organizations will assist them in protecting the privacy of their personal information. Internet users, on the other hand, believe that the same governmental organizations will breach their privacy by revealing personal information without their consent (Turow & Hennessy, 2007).

Numerous studies have demonstrated that a variety of factors affect how Internet users perceive their privacy. Five sets of variables have been the focus of our research in this publication (described above). For the sake of our study, we defined Internet users' perceptions of privacy as their assessment and concern about how a certain website will manage the data that was gathered during their online communications.

3.3.2 Factors that influence Internet users 'privacy concerns - Behavioural Factors

Past studies have concentrated on general consumer concerns about privacy in a variety of circumstances. Culture has been integrated as a demographic aspect in several studies and has

seldom been explored as a cause of privacy concern (Bellman et al., 2004). Others claim that most research on public policy and legal approaches to privacy protection policies was evaluative, looking at the issue from ethical and legal perspectives (Caudill & Murphy, 2000), and focusing on how governments dealt with or should deal with privacy concerns (Clarke, 1999; Pincus & Johns, 1997).

Online privacy concern is described as an Internet consumer's worry about managing the collection and subsequent use of information created or obtained about him or her on the Internet (Castaeda et al., 2007). Castaeda et al. (2007) analyze two dimensions: concern for control over personal information collection and concern for control over its usage on the electronic market. The term "control" refers to cyber security. The term "usage" refers to the insufficient use of information by corporations that have been granted permission to utilize personal data.

A wide range of consumer responses to privacy concerns in general, as well as to online privacy, has been observed. People who profess to be worried about their personal information behave differently when confronted with an information-sensitive circumstance. Some people execute purchases without safeguarding personal information. Some people lie about the information they give to others. Some people avoid information hazards entirely by canceling ongoing transactions. These reactions can be viewed as giving customers more power. Individual behaviors include withholding, protecting, and fabricating.

"Fabricate" refers to consumer attempts to conceal one's identity using fictional or misleading information. The term "protect" refers to the employment of technology to keep prospective attackers out of one's Internet domain. Consumers, for example, can employ technology to refuse cookies. The term "withhold" refers to a consumer's rejection to disclose information or visit websites (Wirtz et al., 2007).

3.3.2.1 Cultural Factors

Because of the relevance of IT application in worldwide and very varied cultural domains, culture has recently garnered increased attention in IS research. Although there are other definitions of national culture, Hofstede's (2001) typology of culture is one of the most broadly applied in a variety of management domains. Most researchers intended to depend entirely on Hofstede's definition. It is plausible that correlations between cultural values and concerns about information privacy exist. For example, studies discovered cultural disparities in information privacy concerns. However, few studies have been done to research how these privacy concerns impact the quantity of Internet and e-commerce use, as well as the relationships between information privacy concerns and cultural values (Milberg et al., 1995; Dinev and Hart, 2006). Numerous academics argued that while analyzing consumers' online privacy concerns, the following three cultural factors should be addressed at a minimum: individualism, uncertainty avoidance, and power distance (Milberg et al., 1995; Dinev and Hart, 2006; Shin et al., 2007).

The hierarchical character of Ghanaian culture runs counter to the very essence of "e-commerce," which requires and undermines hierarchies. One result is that Ghanaians may be less apprehensive about utilizing government and corporate websites that are perceived more "authoritative" than less respectable ones. In terms of uncertainty avoidance, Ghana ranks high, leading to the idea that Ghanaian customers are anxious about unclear situations and unexpected risks such as internet transactions.

Understanding how culture affects technology adoption is critical in the era of technology since it leads to maximizing the utility of new technical innovation. Every culture is unique, and not every technology is equally acceptable or usable in every society. According to Leidner and Kayworth (2006), culture can impact the success of information technology adoption and utilization. Furthermore, such unique cultural characteristics may give some light on the variables influencing IT adoption at the country, community, and individual levels. According

to Al-Smadi (2012) and Al-Hujran et al. (2011) research, Hofstede's cultural dimensions of power, distance, uncertainty avoidance, and individualism/collectivism have a substantial influence on an individual's attitude toward technology adoption in developing countries. Critical literature reveals that technological innovation reflects the developer's culture as well as the cultural demands of the country where it was produced (Al-Smadi, 2012; Karimzadeh and Alam, 2012; Straub, Loch, and Hill 2003). According to Karimzadeh's (2020) research, legal and security difficulties, as well as cultural and managerial banking issues, were drivers influencing the adoption of online transaction services in India.

Surprisingly, Lekhanya (2021) contended that cultural values and traditions had little bearing on internet transactions in South Africa. Moreover, Vatanasakdakul et al. (2004) discovered that the immediate social and cultural expectations of embracing e-commerce in Thailand were the source of their poor acceptance. Thus, the transfer of technology designed within one culture may not be easily accepted or fit in another (Vatanasakdakul et al., 2004), just as Al-Smadi (2012) demonstrated that cultural factors influence the perceptions of culture sensitive people in assessing the usefulness of any technological innovation.

3.3.2.2 Institutional Factors

Institutional variables for consumer online privacy concern and behavior intent typically relate to the regulatory rules and regulations that regulate how various government agencies and other important power holders create Internet privacy legislation and direct and enforce the use of consumer data. In circumstances of power imbalance and data protection concerns, the state is often regarded as having the obligation to guarantee the well-being of consumers (Smith, 1994). Higher degrees of privacy concern, for example, were shown to relate to more mild regulatory settings (Milberg et al., 1995).

Regulation is regarded as critical in preserving internet privacy (Rust et al., 2002). At the industry and organizational levels, privacy policy is concerned with how a company's policy is

viewed by customers in terms of how an industry or business exerts ownership and influence over the use of consumer data. According to Liu and Arnett (2002), just slightly more than half of big corporate websites included privacy policies or adequate links to them from their respective sites. When website administrators create a secure environment, they lessen consumers' privacy concerns and so increase their usage of the site. To preserve consumers' privacy, businesses must safeguard any personal information obtained directly or indirectly from other businesses (Liu & Arnett, 2002).

Perkins and Annan (2021) investigated the elements that drive online banking adoption in Ghana, and their findings found that PU, PEOU, government backing, trust, and security all had a substantial influence on customers' intents to use online banking. As a result, these criteria are critical for considering the launch of online transaction solutions for usage in Ghana.

Ghobakhloo et al. (2020) "investigated the techniques for effective IT adoption in Malaysia and discovered that perceived expenses (software and hardware) and government assistance (legal concerns) affected online transactions among SMEs. Since the study focused on small and medium-sized businesses, most situations and the nature of the firm required an individual to make decisions. As a result, it is possible to conclude that expenses and government assistance influenced the online purchase."

Agwu "investigated the challenges to e-commerce implementation by small and medium-sized firms in Nigeria in 2015. According to the findings, the barriers to e-commerce adoption were lack of a policy framework and knowledge, insufficient skills, and the high expenses of early e-commerce set-up and government support. However, the Internet is not yet an available resource in developing nations in general, and particularly in Nigeria. Because online transactions are a subset of e-commerce, it can be deduced that these problems may also hinder online transaction adoption because only a small number of people in the upper echelons of society can afford Internet access."

According to Fathian et al. (2018), as mentioned in Ghobakhloo et al. (2020), an Iranian government ICT development plan (TAKFA) resulted in a significant increase in IT adoption and e-readiness among Iranian SMEs. As a result, government assistance and individual owners' e-readiness (which reflects on their personalities) influenced the decision to accept and adapt technology use.

According to Zaied (2020), technological challenges, the legal and regulatory framework, Internet security, and the restricted usage of Internet banking all impede the implementation and acceptance of e-commerce among Egyptian SMEs. It may be deduced that a lack of technological and expertise understanding, security, legal and regulatory framework are some critical issues influencing the acceptance of online transactions in Egypt, as online transactions are a part of e-commerce.

Belanche, Casalo, and Flavian (2020) discovered in their empirical study that citizens' personal values and lifestyles influence their decision to adopt e-government in Spain, but they fell short of considering "Personal values and lifestyles" as socio-cultural tendencies that influence their decisions toward e-governance. Adopting this stance, we argue that personal values and lifestyle pertain to socio-cultural values that influence people' decisions to use e-government.

According to “Takele and Sira (2021), the level of online transactions in Ethiopia is still underdeveloped due to a lack of legal and regulatory framework, a high rate of illiteracy, a lack of infrastructure expansion, frequent power outages, and security concerns, which are shared by most African countries. Bultum (2021) also incorporates the legislative framework, national ICT infrastructure, and government backing into the environmental component to investigate the elements influencing online transactions in Ethiopia. The findings found that a lack of a legal framework and regulatory variations are impeding the expansion of internet transactions.

Due to the lengthy history of the empire system of administration in Ghana, Ghanaians tend to reveal their knowledge and observe others' behavior until the entrance of Western culture (EPIC, 2001). Non-jurisprudential systems start to arise. For example, the regulations governing the administration of the supply of internet bulletin board service (2000) are regarded as a more precise legislation on personal data protection than any other in Ghana (Fu, 2002). It requires service providers to keep client information secret and not reveal it to any third party without the consumer's consent, unless compelled by law.

Authorities in Ghana, on the other hand, may use e-commerce development to retain their privileged positions. Surprisingly, it focuses more on safeguarding state property (against below-value expropriation by private concerns) as opposed to private or intellectual rights (Martinsons, 2008). As a result, consumer privacy is less important and sometimes neglected in Ghana. In recent years, the problem of "unauthorized enterprise use of personal information" and the "purchasing and selling" of customer information by firms such as mobile phone providers has grown "epidemic" in Ghana. In fact, according to the most recent poll, "unauthorized use of customer information" was regarded as one of the top consumer protection issues in Ghana. There appears to be an urgent need for government agencies and corporations to take rapid action to secure consumer data and alleviate privacy concerns.

3.3.2.3 Demographic Factors

Age, gender, education level, economic level, and Internet experience have all been linked to differences in online privacy concerns (Graeff & Harmon, 2002; Sheehan, 2002; Bellman et al., 2004). We believe that demographic determinants, while connected to cultural and institutional issues to some extent, are universal. In Ghana, with over twenty million Internet users, most of the population lacks Internet experience, while their educational experience is

limited (GSS, 2018). Also, the central region of Ghana has a greater population than the northern region, and the central economy is more developed.

Additionally, Ameme (2015) investigated the influence of customer demographic characteristics on Internet banking acceptance and use in Ghana and discovered that demographic variables such as gender had no significant effect on Internet banking service adoption.

Tarhini et al. (2015) used a qualitative method to investigate user adoption of internet banking in Nigeria. According to the survey, security is a crucial predictor of online banking uptake. Additionally, the report discovered that culture and religion had an impact on internet banking acceptance.

Polasik and Wisniewski (2019) investigated the factors that influence the decision to adopt online banking in Poland and discovered that perceived level of security, as well as demographic variables such as age, gender, previous experience with self-service technology, and educational level, had a significant effect on attitude toward online banking adoption. This survey did not focus on the issues of trust and privacy that customers are concerned about. Customers' trust will be destroyed if sufficient security and privacy protection are not provided, which may hinder the adoption of the international business platform. Chong et al. (2018) investigated the factors that influenced the choice to use internet banking in Vietnam. The effects of PU, PEOU, trust, and government backing on online adoption were investigated. According to the findings, PU, trust, and government support were all positively related to the desire to utilize internet banking in Vietnam. In contrast to TAM, PEOU had no relevance in the investigation. Additionally, the findings demonstrate that trust in security and privacy affected online banking uptake in Vietnam.

Izogo et al (2020) conducted a study on the impact of demographic variables on consumers' adoption of online transactions, finding that marital status, age, and educational level have a

major impact on online transaction adoption in Nigeria, but gender, religion, and income have no significant impact.

Al-Hujran et al. (2020) investigated national culture's influence on citizen acceptance of electronic government services, discovering that power distance and uncertainty avoidance had substantial effects on individuals' intents. Additionally, the PU, PEOU, and attitude of individuals were strong predictors of their desire to use state government online services. Remaining in Jordan, Al-Majali and Mat (2020) used IDT to investigate the causes of Internet banking service uptake. Their research demonstrated that PEOU, PU, compatibility, trialability, trust, and awareness all have a major impact on Internet banking uptake. These findings suggest that they are crucial factors of clients' international business adoption in Jordaan.

Odior and Banuso (2020) investigated the difficulties, advantages, and policy implications of cashless banking in Nigeria. The study identified infrastructure deficiency, unreliable power supply, inadequate literacy level, religious views, security, and lack of trust as factors influencing the adoption of internet transactions in Nigeria.

Moreover, Yaqub et al. (2021) investigated the cashless policy and revealed that the constraints of customers' acceptance of the online transaction platform include security, infrastructure, legal and regulatory concerns, as well as socio-cultural issues. Surprisingly, these writers (Odior and Banuso, 2020; Yaqub et al., 2021) ignored the importance of supporting their statements with scientific evidence.

Odumeru (2020) used a modified TAM in which PU was substituted by perceived advantages to explore the adoption of online transactions by customers in Nigeria. The conclusion of the investigation demonstrated that adoption of online transaction in Nigeria is impacted by age, educational background.

Haq and Khan (2021) used chi-square to investigate the influence of demographic characteristics on the adoption of online transactions in India and discovered that demographic parameters (age, income, education, and occupation) had an impact on online transaction adoption.

As a result, Muzividzi et al (2021) stated that typical Internet banking users were young, rich, and well educated. Non-adopters cited a lack of understanding of the operation of the online transaction system as the explanation for their failure to comply with the service.

Muzividzi, Mbizi, and Mukwazhe (2021) discovered that security, lack of understanding, and lack of Internet skills were key variables affecting Internet banking acceptance among intellectuals in Zimbabwe. According to the survey, young males who were well-educated and made an above-average salary were more likely to use Internet banking than females.

Fonchamnyo (2021) used extended TAM to investigate the causes of customers' perceptions of online transactions in Cameroon. Customers' attitudes regarding online transaction adoption were significantly influenced by perceived security, trust, cost of service, usefulness, and accessibility, according to the findings. Age, education, and marital status were also shown to have a significant impact on attitude, whereas perceived dependability, trust, security, and accessibility had a substantial impact on the Probability of online transaction adoption. In addition, income, perceived benefits (PU), PEOU, perceived risk, and reported enjoyment are also factors.

Egbo et al. (2020) examined 415 undergraduate students' gender perceptions and attitudes regarding e-learning in Ghana and discovered that gender had no considerable influence on e-learning adoption. In contrast, the article ignored the influence of culture on individual attitudes in the e-service context.

3.3.2.4 Perceived Privacy Risk

The internet has enabled us to conduct business with people who live thousands of kilometers away while also bringing cyber criminals. The vast majority are the consequence of unlawful and fraudulent usage of personal identifiable information. People's worry about privacy grows as personal details (like credit card numbers and bank account details) is misused. Others have stated that, while people may regard the Internet as a marketing tool, security and privacy concerns have a significant impact on online purchasing decisions (Smith and Rupp, 2002). Considering the rise of online identity theft and identity fraud, a person's level of worry about online privacy will impact how they view a specific privacy issue (Cockcroft et al., 2005).

Ong and Lin (2015) investigated security, risk, and trust in Taiwanese Internet banking adoption and concluded that perceived security is a predictor of trust and perceived risk. According to the study, perceived security has both direct and indirect implications on people's adoption of Internet banking. When Selvanathan et al. (2016) investigated Internet banking problems among Malaysian clients, they discovered that pricing, security, and PEOU had a positive association with Internet banking adoption, while resistance to change was minor.

Previous research by Dixit and Datta in 2018 on "acceptance of online transactions among adult customers: an empirical investigation in India" using descriptive statistics, factor and regression analyses yielded the following results: security and privacy (=0.477), trust (=0.246), innovativeness (=0.272), familiarity (=0.589), and awareness (=0.243). In other words, adult clients are more likely to use online transaction services. Gilaninia et al. (2020) investigated the effective factors influencing customers' trust in online transaction services and discovered that perceived security, perceived usefulness, perceived privacy policy, and customer satisfaction were critical determinants that positively influenced customers' trust level to adopt the technology in Iran. Furthermore, the authors claimed that these characteristics ensured customers' faith in their accounts, which enhanced their trust in online transaction services. In other words, the service providers' understanding of trust and security in online transaction

technologies should increase customers' faith in e-transactions. Gilaninia et al. drew their conclusions using both correlation and multiple regressions. On a different level, Khaledi et al (2020) investigated the elements that impacted customers' use of a bank's e-services and discovered usefulness, ease of use, pleasure, information security, confidentiality, and Internet quality to be strong predictors of customers' trust in online transaction usage. Kim et al. (2018) discovered that perceived security (= 0.419, t = 3.012, p 0.01) and perceived trust (= 0.297, t = 3.835, p 0.01) in e-payment use are also significant.

Aliyu, Younus, and Tasmin (2020) investigated the adoption of online transactions in Nigeria to identify consumer behaviour and critical success factors in Nigeria. The findings revealed that awareness, security, cost, and accessibility are all crucial factors in online transaction adoption in Nigeria, but perceived ease of use and reluctance to change were found to be insignificant.

Akanbi, Ayodele, and Adedipe (2021) investigated the factors influencing undergraduates in Nigeria's intention to use Internet banking. They discovered a positive significant association between ability, capacity, compatibility, perceived risk, PEOU, and PU and the propensity to utilize Internet banking.

Special privacy hazards exist in Ghana due to governmental policy, the rule of law, and the execution of the law. For example, the "human flesh search engine," a literal translation of Ghana, is a phenomenon in which the Internet populace is mobilized to locate certain persons or facts. Most Ghanaian Internet users are aware with the word, since the engine has lately been utilized to locate and penalize persons who are suspected of publishing improper items. Personal information about those persons might be posted on the Internet in most situations. Those who were exposed online regarded it as a terrible infringement of their privacy in certain situations. A debate has emerged recently regarding whether the country should issue suitable privacy legislation or guidelines to restrict the use of the "human flesh search engine".

Hashjin, VakilaRoaia, and Hemati (2021) investigated the determinants influencing Internet banking acceptability in Iran province, employing integrated variables from TRA, TPB, TAM with trust and security, government support, and demographic data. PEOU, PU, Subjective norms, behavioral intention, attitude, trust, and government backing were revealed to have a substantial influence on Internet banking adoption.

In Ghana, sharing personal information online may also be dangerous. For many online purchases, it must supply national identity card numbers. This creates serious privacy concerns. Certain sensitive and confidential information gathered and stored by governmental entities appears to be available to individuals with good guanxi. As a result, customer information is routinely exchanged and misappropriated in Ghana. As previously said, this has become a major issue. Ghanaian top-level domains are typically seen as less secure in terms of technology and infrastructure.

In 2020, Juwaheer et al investigated the factors that drove the embracing of Internet banking in Mauritius and concluded that trust and security were the most important predictors of online transaction adoption in Mauritius.

According to Sohrabi, Yee, and Nathan (2021), stronger security and privacy standards in the banking sector can increase client trust in online transaction acceptance. In 2021, Hong et al. investigated the variables influencing Internet banking adoption in Malaysia, finding that complexity, security, and customer experience (Internet Usage) had a major effect on adopters. Individual factors (demographic variables) were discovered to have an insignificant impact on adoption. In Pakistan, Kazi (2021) discovered that PU has a considerable influence on Internet banking adoption, but that PEOU is minor.

Maduku's (2021) investigation into the predictors of retail banking customers' attitudes toward Internet banking adoption in South Africa using extended TAM integrated with trust, subjective norm, and demographic variables revealed that PU, PEOU, and trust had a strong significant

relationship with attitude, whereas demographic variables such as age, income, and education had a weak and poor relationship with customers' attitudes towards Internet banking adoption.

Many research, both in developed and developing countries, have been undertaken to uncover numerous characteristics that impact online transactions. Yet, the characteristics required for online transactions are continually growing, and this reality requires greater examination. Ayo, Adewoye, and Oni (2018) investigated the state of international business implementation and e-payment adoption in Ghana and discovered that perceived ease of use (PEOU) and perceived usefulness (PU) are not only preceded by acceptance, but also key determinants of customer retention in the international business system.

According to Al-Smadi (2020), in Jordan, uncertainty avoidance of culture was discovered to be the major cultural factors that have a strong positive and significant impact on PU and PEOU; however, perceived risk was discovered to have a strong impact on customers' attitude, which influenced customers' intention to use online transaction services.

Nevertheless, Eze et al. (2020) researched the elements that influenced Internet banking adoption among Malaysian young adults and discovered that PU and PEOU are among the characteristics that influence consumers' acceptance of international business initiatives. It could be deduced that the study helped bank managers to grasp community peoples' behaviour towards international business decisions, while also implementing essential methods to encourage the community to accept, adapt to, and employ the innovation.

Nasri analysed the factors impacting Internet banking penetration in Tunisia in 2020. The author concluded that security, prior knowledge of Internet use, and risk are drivers of Internet banking adoption in Tunisia. Surprisingly, the author overlooked the significance of trust in a fraudulent atmosphere. According to Omar et al. (2020), clients in Pakistan favoured Internet banking over traditional banking owing to its dependability, convenience, speed, trust and security, cost efficiency, user-friendliness, and error-free system. Customers' adoption

decisions are influenced by security concerns, a lack of trust, and a lack of awareness about Internet banking services, according to the authors. Yet, according to Gilaninia et al (2020), perceived security, perceived privacy, perceived usefulness, and customer happiness are crucial factors in increasing international business adoption. According to the findings of Kumar, Sareen, and Barquissau (2020), the amount of adoption of international business systems is positively associated to the level of individual confidence in the banking environment. Security, accompanying guarantees, service excellence, and benign attributes can all impact confidence.

3.4 Concept of Risk Management in Online Transaction

Fraud detection and prevention are not a one-time task (Dimitrijevic, et al., 2015). Rather, it is a continuing process that mainly embraces monitoring, decision making, irregularity exposure, case management as well as realizing to feed upgrading in detection back into the system (Data Security Council of India, DSCI, 2020). The security and dependability of information, accounts, assets, and transactions associated with customers and businesses are to ensure to employ an effective fraud detection program. Putting up an effective fraud risk management program necessitates thorough grasp of how and why fraud is perpetrated (CIMA, 2009). The fraud risk is just one of many kinds of risks an organization manage. Bereft of well-defined, clear objectives, a fraud risk management program cannot be successful (DSCI, 2020). An effective fraud risk management program foundation is a sophisticated and rigorously implemented fraud risk assessment. In managing the fraud risk, the use of automated uninterrupted monitoring tools is the safest practice. If, however, not well implemented it can turn out to be time consuming and cumbersome (ACFE, 2020).

Risk management involves a process of proactively and analytically identifying, evaluating, and assessing risks on continuing basis and drawing out plans and activities for risks handling (DSCI, 2020). This task is as normal carried out by businesses that are seeking to proactively

improve their posture towards risks and prevention of threats. Risk management is process that involves identification, assessment and ranking of risks followed by coordinated and economical resources application to curtail, monitor, and curb the probability or impact of calamitous incident (Hubbard, 2009) or to maximize the opportunities realization. Risk management assists firms identify budding risks, vulnerabilities, and threats which when reached might immensely impair the interest of firm. The firm then appraises its occurrence likelihood and applies controls to deal with the risk. The handling could be to transfer, mitigate, accept, or avert the threats, depending on the risk tolerance, and return of investment for firm's business interest. Process such as this in retail payment transactions assist to avert frauds and allied swindles. This in payment industry is a de-facto benchmark among organizations (DSCI, 2020).

3.5 Risk Management in Emerging Retail Payments

These modern payment systems, which are related to computer technology, telecommunications, and online transactions, rely on electronics for virtually all or all their activities. Several products based on these payment systems have failed outright, while others have struggled to sprout and a few have become widely accepted in regular transactions (Braun, McAndrews, Roberds, & Sullivan, 2008). Every single one of them is exposed to a range of dangers. Learning about these hazards, news bulletins on data violations, identity fraud, and frauds have all become a part of the electronic payment environment. Novel aspects associated with "emerging" payments include low-cost data collection and transmission methods. Such technologies can reduce risk, but they can also introduce new dangers (Braun et al. 208). It is about time to create a framework and vocabulary to examine how innovative payment technologies effect risk, particularly in many ways to make noncash payments as payments shift from printed to electronic form (Federal Reserve System, 2004).

Cybercrime is a risk that is carried out by the reckless behaviour of computer and internet users who take advantage of weaknesses in computer networks and the internet medium to perpetrate fraud (Bendle, 2019). Cybercrime is frequently carried out by organized cliques (Levi, 2018), with the potential to wreak massive damages. Moreover, Hawkins, Yen, and Chou (2018) contend that the openness of the Internet medium, which provides access, opens the medium for criminal acts. Furthermore, the anonymity of the Internet conceals the intents of cyber-fraudsters (Laudon & Traver, 2016), making it more difficult to manage cybercrime operations. Commercial transactions centred on internet applications provide several dangers or hazards to both customers and merchants, if necessary, security measures are not appropriately implemented (Patel, Patel, Patel, & Pathrabe, 2017). Loss of money through online transactions because of cybercrime impacts both businesses and customers. Moreover, Boateng, Molla, Heeks, and Hinson (2020) suggested that cybercrime operations have the potential to stymie progress in less developed countries.

Electronic financial transfers, deceptive internet sales, identity theft, phony investments, and advance payment schemes are all examples of crimes committed via the Internet (Clough, 2010). Many individuals are concerned about the risk of e-commerce company transactions because of cyber-fraudsters' activity. Yet, for effective corporate online transactions, processes must be implemented to guarantee the security of both the firms and the customers (Apau, Nti, & Adu, 2019). Many less developed countries have made significant efforts to adopt e-commerce technologies. Yet, malicious computer users continue to use Internet and computer network weaknesses to commit crimes against users (Warner, 2011). Cybercriminals uncover flaws and vulnerabilities in e-commerce technology, exploit the flaws, and exploit victims using a variety of strategies (Patel et al, 2017).

Understanding the risk structure is beneficial, but analysing deaths and mitigation attempts in a unique payment product can be difficult. Little fraud losses, for example, might imply that:

1) the risk is modest, 2) existing mitigation techniques are effective, or 3) faults have not yet been identified (Braun et al., 2018). Large levels of loss, on the other hand, show that the risks are significant, and it may take some time to determine whether mitigating measures can be done. Only time and problem monitoring will reveal whether risk can be managed in either case. In this evaluation, it is being assessed if, during this phase of uncertainty, an emergent payment method promoter has sufficient incentives and instruments to reduce risk before the fatalities from fraud or operational troubles becomes common (Federal Reserve System, 2004). According to this evaluation, promoters and providers of efficient new payment systems must be cognizant of potential fraud risk as well as operational risk. Furthermore, businesses are obligated to reduce these risks or face exclusion from the payment industry. Service providers of new payment systems can manage risks by restricting access to their payment networks, verifying compliance with risk mitigation criteria, and imposing noncompliance penalties (Braun et al., 2018; Hewitt, 2020). According to Braun et al. (2018), while most of this control work is voluntary, some is mandated by governmental agencies charged with coordinating operations as well as defining and enforcing rules.

This review goes into the structure and vocabulary of growing payment method hazards and their mitigation through various approaches. It begins with a description of several fraud and loss instances involving developing payment mechanisms. The analysis then describes an economic framework for valuing risk control in retail payments. In addition, the framework's application to three additional payment forms' risk episodes. The accounts that follow reveal fraud and operational challenges that took advantage of new payment system features. A telemarketing fraud, a sophisticated web fraud, and two data security infractions were among the instances examined. The crimes that caused these instances, such as con artistry, fraud, deceit, and stealing money, assets, or someone's reputation, are not new. Therefore, the

operational issues are not novel; rather, the expected scope and quickness of disruptions are of a magnitude atypical of their paper-based counterparts.

i. Telemarketing Fraud

The Federal Trade Commission (FTC) announced in 2012 that it had shut down the Assail Telemarketing Network and its subsidiaries. According to the FTC, the Assail firms engaged in telemarketing activities from claimed confidence trick operations that provided credit cards to customers with poor credit histories (FTC, 2005). Under the guise of collecting affiliation fees, these firms persuaded customers to provide the bank and account information from their cheques (Braun, McAndrews, Roberds, & Sullivan, 2008). Telemarketers then used this information to create electronic debits to customers' checking accounts as payment for the "affiliation" dues. These credit cards appear to have been sent seldom, if at all. But the customers discovered that they had also been subscribed for high-priced and uncertain items (alleged high-order schedule), such as motor club memberships, the dues for which were specifically paid to their check accounts. When customers complained, the companies used complicated routines to evade refunds or affiliation revocation. According to the FTC, assail and its directors participated in deceptive marketing operations totalling more than one hundred ($00) million dollars (Braun et al., 2018).

Assail's electronic transaction type was debit via the automated clearinghouse (ACH), which had to be processed, received, and distributed by participating banks. Participating banks are expected to monitor the firms for which they provide this ACH start service. About this incident, First Premier Bank admitted that it had failed to do due diligence on the clients' validity and activity, but at the time it aided in identifying the telemarketers and providing important evidence to the fact-finding agencies. After that, the bank paid $20,000 to South Dakota, Iowa, and Minnesota in exchange for a broader settlement and agreement to actively engage in know your customer (KYC) practices as well as ongoing surveillance of client

behaviour (FTC, 2005). Prior to the adoption of this ACH transaction type by Assail, this sort of fraud was routinely accomplished by producing "remotely created cheques," which had a written legend in place of the payer's signature. Such a ruse is still used to commit fraud, but it does not deliver the speed and scale that this imposter achieved using automation (Federal Reserve Board, 2006).

ii. Transaction Fraud and Data Security Breach

In the year 2018, the United States Department of Justice reported that two Russian men, Alexey Ivanov and Vasiliy Gorshkov, used unofficial access to Internet service providers in the United States to steal bank account, credit card, and other private financial information from over fifty thousand (50,000) people (U.S. Department of Justice, 2002). They infiltrated computer networks and then used the stolen processors to commit fraud through PayPal and eBay, an online auction website. According to Justice Department news releases, the impostors used byzantine programs to build up thousands of shady e-mail accounts on websites that did not have high-tech systems capable of detecting human intervention at the time. Gorshkov used the algorithms to establish PayPal accounts based on random personalities and stolen credit card information. Following that, the programs transfer monies from one account to another to generate cash and pay for computer equipment purchased from US providers. Another computer application allowed the collaborators to handle and manipulate eBay auctions in such a way that they could function as both retailers and successful bidders in the same auction and then successfully pay themselves using the stolen credit cards (Physor.com, 2006).

This was imposters hacking into databases, stealing payment-related and additional information, using the stolen identities to create phony accounts, navigating online auctions, and using machine-based tools to spread their crimes and confuse the audit/transaction path. Finally, the FBI used a covert method to get the two hackers to Washington, inviting them

under the premise of a job interview with "Invita," a fabricated computer security business. In October 2020, the two guys were sentenced to three years in jail.

iii. Unsecure Data

The president and chief executive officer of Card Systems Solutions, Inc., a transaction processor, testified before a Congressional committee in 2015 that, in September 2012, an unauthorized party installed an undercover computer program on a company's transaction processing system (Perry 2015). Card Systems announced on May 22, 2015, that it had faced a "possible security skirmish." Account numbers, account holders' names, expiry dates, and security codes were stolen from records on two hundred sixty-three thousand (263,000) transactions. A total of forty million (40,000,000) records were potentially at danger. Card Systems reported breaches to its bank as well as MasterCard, American Express, and Visa. These three credit card companies determined that Card Systems violated the credit card industry's data retention regulations as well as current security. Visa and American Express said that they would not allow the firm to handle their transactions after October 3, 2005. Pay by Touch announced its Card Systems Solutions purchase on October 5 because of the company's network connections to 20,000 merchants, notwithstanding the failure of its card transaction processing operation (Pay by Touch, 2005).

TJX Companies, which runs stores in Ireland, Canada, the United Kingdom, and the United States disclosed in early 2017 that data security breaches from mid-2015 to late 2016 may have jeopardized over forty-five million shopper information (TJX Companies, Inc., 2007). Similarly, the company's investigations uncovered vulnerabilities and putting driver's license addresses and numbers at jeopardy. The Massachusetts Bankers Association reported fraudulent use of credit and debit cards issued by its members because of the incident. According to the Association's press releases, fraudulent card data was used to make payments in many US states, Sweden, Hong Kong, and other countries (Massachusetts Bankers

Association, 2007). According to the Wall Street Journal, hackers first intercepted data transmissions from handheld devices used to manage shop inventory and prices (Pereira J., 2007). They used the acquired data to crack encryption protocols and steal usernames and passwords from corporate headquarters workers. After their access into the TJX network, they stole debit and credit card details and even left messages for each other. The numbers of the allegedly stolen cards were then reportedly sold on the Internet. Press stories follow down bank deaths around the country. In addition to direct transactions with stolen debit and credit card details, the intruders or their clients purchased prepaid cards, which were then utilized to purchase goods and services.

Table 1: Summary Table

Author(s)	**Title**	**Factors**
Ayo, Adewoye and Oni (2018)	Online Shopping and Customers' Satisfaction in Lagos State, Nigeria	investigated the state of international business implementation and assessed trust in e-payment adoption in Ghana and discovered that perceived ease of use (PEOU) and perceived usefulness (PU) are not only preceded by acceptance, but also key determinants of customer retention in the international business system.
Auta (2018)	International Business Adoption	Access and information scarcity were major concerns for international business adoption.

Eze et al. (2020)	Perceived Ease of Use (PEOU) and Based on behavioural Intension to Use (BIU): Mediating influence of Attitude toward Use (AU) with reference to Mobile wallet Acceptance and Adoption in Rural India.	The perceived utility (PU) and perceived ease of use (PEU) (PEOU)
Al-Hujran et al. (2020)	The influence of power distance and the avoidance of uncertainty on the adoption of electronic government services.	power distance and uncertainty avoidance
Omar et al. (2020)	Factors that influence the use of E-wallet among students	Reliability, convenience, speed, trust and security, cost effectiveness, user-friendliness, and an error-free system are all important considerations.
Gilaninia et al (2020)	The Effects of Perceived Security, Trust, and Information Quality on Mobile Payment Usage via Near-Field Communication (NFC) in Saudi Arabia	Customers' pleasure, perceived security, perceived privacy, and perceived usefulness

3.6 Summary of main findings

Many studies have been conducted to study consumers' perceptions and behavioural intentions about internet privacy and security. However, the primary factors remain ambiguous,

which may be owing to the changing nature of emerging technology. When in Ghana, it might be due to social, cultural, and economic differences. Additionally, there have been few empirical research in Ghana that have studied the models of users' attitudes and behavioural intentions about online privacy and security. This study seeks to bridge that knowledge gap by concentrating on the best model for online privacy and security.

Practical Part

4.1 Research questions

RQ1: What factors influence perceptions and behavioural intentions of online buyers in Ghana?

4.1 Research Design

Creswell & Creswell (2016) define three research approaches: (a) qualitative, (b) quantitative, and (c) mixed techniques. Three key contrasts between quantitative and qualitative research methodologies are identified by Saunders et al. (2016). The authors' first point of distinction is that the quantitative research approach allows the researcher to isolate and identify variables before linking them together to form research hypotheses. This is not the case with the qualitative research method. The authors say that the quantitative research approach provides for impartiality in terms of the procedures involved in data collecting and analysis. Subjectivity, on the other hand, is frequently introduced throughout data collecting and processing techniques in qualitative research. Lastly, whereas quantitative research allows for the use of bigger samples and the generalization of sample results to the entire population, the goal of qualitative research is not to extrapolate sample findings to the entire population.

This research, "As a result, a mixed research approach was used in view of the purpose of study, specific objectives, and the essence of the primary and secondary data that was gathered and studied. According to Creswell (2014), a mixed approach focusses with explaining phenomena through gathering numerical data and analysing it using techniques based on mathematics (statistics)."

4.2 Population of the Study

The population of the study was centred on Ghanaians who uses the online platform for their transaction. The total number of populations was thirty-one million respondents.

4.3 Sampling Procedure and Sampling Size

Sampling refers to the art of selecting a set of respondents out of a population who share the same characteristics of the population of the study such that the information derived from the sample cam be used to represent the whole group. For the purposes of the study, the researcher selected individuals who purchases and pay for their transaction using their credit cards. Researchers such as Field (208) and Walubwa (2020) have argued that if the population is unknown, a minimum of 384 responses are sufficient if confirmatory factor analysis (CFA) or Structural equation model (SEM) is applied later for data. Since this study will use the confirmatory factor analysis (CFA), a sample of 390 respondents which more than satisfies the minimum requirement. In view of this, the sampling technique will be used.

4.4 Data Collection and Analysis

4.4.1 Types and Source of Data

Data source refers to the various avenues through which data is derived for a research study. For the purposes of this study, the researcher sampled primary sources and secondary source of data. Thus, with the help of questionnaires, and secondary data from the various online trading platform, primary data through question and secondary data by downloading the news items which were published online relating to privacy and online security. Also, existing articles and literature would be used to justify and explain the study findings. The link between the current study results and the previous studies results would be compared and differentiated.

4.4.2 Methods of Data Collection

Based on the busy schedules of the respondents and difficulty in accessing the respondents physically, the study employed the use of google documents form to collect the data from the respondents. Being that the data to be collected were done using standardized instruments, it was easy to translate these into google documents form for respondents to respond to them at

their convenience. The data was collected from the 13th of November 2022 to the 20th of December 2022.

4.4.3 Instruments for Data Collection

Closed-ended questions were used in the study to elicit data from respondents. Because the study's goal was to obtain quantitative data, questionnaires were used. This was due to the ease with which quantitative data could be acquired and examined. Again, the researcher verified that quantifiable data was acquired using questionnaires. Based on the study aims, the questionnaires were separated into numerous subheadings.

This was done to allow for additional specificity while also ensuring that the data gathered was relevant to the research topic. Based on this, the first section of the questionnaire focused on the respondents' demographic characteristics. Following that, the next section of the questionnaire focused on the risk associated factors in the organization's online insurance. The concluding section of the questionnaire was designed to elicit information on businesses' ecommerce patronage. After the construction of the questionnaire, it was compared to the findings of previous empirical investigations. Moreover, it was contrasted to what the literature had to say about risk in online insurance and ecommerce patronage.

4.4.4 Data Analysis

The Structural Equation Model was used in the study to analyse the objectives. The study's initial goal was to examine the models that impact the privacy and security of internet enterprises. This was chosen since the research was conducted quantitatively. To begin, descriptive statistics were utilized to assess and report the respondents' age, gender, level of education, and marital status. The regression analysis was also utilized to examine the influence of user perception elements on online privacy and security, as well as behavioural intents on online privacy and security. Prior to this, the Cronbach alpha test of reliability was used to establish if the data obtained from the field was dependable for further research. Again, when

the regression analysis was completed, the researcher checked the data for normality. To meet the study's aims, three models were proposed to investigate the relevant existing models of online privacy and security.

4.4.5 Models

The first model was to analyse the effect of user perceptions on privacy and security online. The literature review identified series of factors that influence privacy and security online. Three main set of models were identified and explained.

Model 1 - cultural factors, institutional factors, demographic factors, and perceived privacy risk on privacy and security online

The first existing model was the relationship of cultural factors, institutional factors, demographic factors, and perceived privacy risk on privacy and security online. The first model is presented on equation 1.

$$PSO = \alpha + \beta_1 CF + \beta_2 IF + \beta_3 DF + \beta_4 PPR + \varepsilon \dots\dots\dots\dots\dots\dots (1)$$

PSO – privacy and security online

CF - Cultural Factors

IF - Institutional factors

DF - Demographic Factors

PPR - Perceived Privacy Risk

ε – error term

Model 2 - customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship and legislation and government privacy protection on privacy and security online.

The second model had relationship between customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship and legislation and government privacy protection on privacy and security online.

$$PSO = \alpha + \beta_1 CIC + \beta_2 SF + \beta_3 WC + \beta_4 CWR + \beta_5 LGPP + \varepsilon \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

PSO – privacy and security online

CIC - customer-intrinsic characteristics,

SF - situation factors,

WC - web site characteristics,

CWR - customer and web site relationship, and

LGPP - legislation and government privacy protection.

ε – error term

Model 3 - control over information and usage of information, short term transaction and established relationships on privacy and security online

The third and final model had variables such as control over information and usage of information, short term transaction and established relationships on privacy and security online.

$$PSO = \alpha + \beta_1 CoI + \beta_2 STT + \beta_3 ER + \varepsilon \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

PSO – privacy and security online

Col - Control over information collection and usage of information,

STT - Short-term transaction,

ER - Established relationship

ε – error term

4.5 Validity and Reliability of Data

The degree to which measuring equipment deviate from random-error variance is measured by reliability (Hayes, 206). According to Egyiri (205), random mistakes might impair measurement reliability, resulting in the assessment of constructs that differ from the constructions intended to measure. In this study, the Cronbach's alpha estimate was employed to determine test-retest reliability as well as internal reliability. Internal reliability is concerned

with the amount to which the elements that comprise a scale measure the same thing; otherwise, the final score is useless (Egyiri, 2015). Face validity was determined by confirming that the questions on the study's instruments contained statements that tested the different traits meant to be measured. Additionally, by enabling my supervisor to examine the authenticity, the content validity of the instruments was confirmed. The researcher used a twelve-day delay to ensure that respondents were not too acquainted with their past replies, which might assist determine whether they comprehended the questionnaire well. The questionnaire was sent over a three-week period. This is required to determine whether the elements on the scale are comprehended in this context.

5.0 Results and Discussion

This section examines the study's aims. The study presented three models for predicting internet privacy and security. The first model investigated how cultural, institutional, demographic, and perceived privacy risk effects online privacy security. The second model considered customer intrinsic traits, scenario aspects, website characteristics, the interaction between the client and the website, as well as legislation and government privacy protection. The third model included control over information collection and utilization, short-term transactions, and established relationships to be variables impacting online privacy and security. The chapter began with a discussion of the respondents' demographic characteristics. Each variable's reliability and validity were investigated and evaluated.

5.1 Results

5.1.1 Demographic Characteristics

This section analysed the demographic characteristics of the respondents. The table from the results is presented below.

Table 2: Demographic Characteristics

Variable	Frequency	Percent
Gender		
Female	185	47.4
Male	205	52.6
Age		
25-30	68	17.4
31-35	54	13.8
36-40	50	12.8
41-45	60	15.4

46-50	59	15.1
51-55	48	12.3
56-60	51	13.1
Education		
Diploma	64	16.4
HND	55	14.1
Undergraduate Degree	58	14.9
Masters	51	13.1
Doctorate	67	17.2
Other professional qualification	95	24.4
Household Income		
Less than 1000 cedis	139	35.6
1001-5000	128	32.8
More than 5000	123	31.5
Experience on Trading Platform		
1	94	24.1
2	76	19.5
3	76	19.5
4	73	18.7
5 and more years	71	18.2
Total	390	100.0

Source: Author's Field Survey (2022)

From Table 2, out 390 respondents for the study, 205 were males which represented 52.6 percent of the respondents. One hundred and eighty-five (185) of the respondents were females which also represented 47.4 percent of the respondents. With respect to the age, respondents

between the ages of 25-30 years were 68. This represented 17.4 percent of the respondents. Respondents between the ages of 31-35 years were 54. This also represented 13.8 percent of the respondents. Respondents between the ages of 36-40 years were 50. This also represented 12.8 percent of the respondents. Respondents between the ages of 41-45 years were 60. This represented 13.1 percent of the respondents. Respondents between the ages of 46-50 years were 59. This represented 15.1 percent of the respondents. Respondents between the ages of 51-55 years were 48. This represented 12.3 percent of the respondents. Respondents between the ages of 56-60 years were 51. This also represented 13.1 percent of the respondents.

With respect to the educational background, 64 of the respondents were holding diploma. This represented 16.4 percent of the respondents. Fifty (55) of the respondents were holding HND. This represented 14.1percent of the respondents. Fifty-one (51) of the respondents were holding master's certificate. This presented 13.1 percent of the respondents. Sixty-seven (67) of the respondents were holding doctorate degree. This represented 17.2 percent of the respondents. People with other qualification were 95. This represented 24.4percent of the responds.

The data on household income showed that, 139 of the respondents were earning less than 1000 cedis. This represented 35.6 percent of the respondents. One hundred and twenty-eight (128) respondents were earning between 1001 and 5000 cedis. One hundred and twenty-three (123) of the respondents were earning more than 5000 cedis. This also represented 31.5 percent of the respondents. Ninety-four (94) of the respondents had 1 year experience. This represented 24.1 percent of the respondents. Individuals with 2-year and 3-year experience with training platform were 76. This represented 19.5 percent of the respondents. Seventy-three (73) of the respondents had 4-year experience. This represented 19.5 percent of the respondents. Finally, 71 of the respondents had 5 and more years' experience on the trading platform. This represented 18.2 percent of the respondents.

5.1.2 Reliability and Validity Test

In research initiatives, reliability and validity are important in determining the degree to which measuring scales are valid and trustworthy. The Cronbach Alpha test was employed to assess the internal consistency of the structures. The permissible Cronbach Alpha test rate was 70% (0.7), and any construct recorded below this level implies poor internal consistency (Christmann & Van Aelst, 2006). The factor analysis was used to examine the reliability and validity of the items measuring the constructs. Items that scored less than the specified criterion (0.6) were removed from the construct. The Cronbach alpha was also employed to assess the constructions' reliability. In the regression model, constructs with loads greater than 0.7 were considered dependable. The individual constructs' reliability and validity are discussed in depth below.

5.1.2.1 Validity and reliability results for Cultural Factors

In assessing the construct, three elements were used to measure cultural factors. After the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (.653), determinant (.025) and Bartlett's Sphericity Test ($X^2(3) = 222.562$; $p<0.05$) assumptions were met, factor analysis was conducted on all three items. The three components used to measure the construct were highly loaded (>.5). On the three (3) items using the Cronbach Alpha, reliability tests were carried out. Cronbach's Alpha was registered at .903. This suggests that the three elements were accurate in measuring cultural factors variable. The naïve method was used to measure the cultural factor variable.

Table 3: Exploratory Factor Analysis on cultural factors

	Factor Loading
In my culture, there are a few things one isn't required to buy online.	0.754
The individuals who impact my conduct accept I ought to not utilize the online exchange items and services	0.842
I think clients ought to not address the banks' director almost the online exchange items and services.	0.785
Cronbach Alpha	**0.903**
Eigenvalue	**3.363**
% of Variance	**67.26**
KMO=0.653; χ^2=222.562; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.2 Validity and reliability results for institutional factor

Three criteria were employed to quantify institutional characteristics in analysing the concept. After meeting the Kaiser-Meyer-Olkin (.632), determinant (.025), and Bartlett's Sphericity Test (X2(3) = 279.960; p0.05) assumptions, factor analysis was performed on all three items. The three components utilized to calculate the construct's load were all significantly loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was.919 at the time. This implies that the three components accurately measured the institutional factors variable. The institutional factor variable was measured using the naive technique.

Table 4: Exploratory Factor Analysis on institutional factors

	Factor Loading

I accept that security seal of endorsement programs such as TRUSTe will force sanctions for online companies' noncompliance with its security approach.	.709
Security seal of endorsement programs such as TRUSTe will stand by me in the event that my individual data is abused amid and after exchanges with online companies.	.834
I am sure that security seal of endorsement programs such as TRUSTe can address infringement of the data I gave to online companies.	.870
Cronbach Alpha	**0.919**
Eigenvalue	**3.788**
% of Variance	**75.76**
KMO=0.632; χ^2=279.960; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.3 Validity and reliability results for demographic factors

Three items were employed to quantify demographic characteristics while evaluating the concept. After meeting the Kaiser-Meyer-Olkin (.706), determinant (.007), and Bartlett's Sphericity Test (X2(3) = 357.777; p0.05) assumptions, factor analysis was performed on all three items. The three components utilized to calculate the construct's load were all significantly loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.945. This implies that the three parts correctly measured the variable demographic characteristics. To measure demographic characteristics, the naive technique was utilized.

Table 5: Exploratory Factor Analysis on demographic characteristics

	Factor Loading

I consider myself as an awfully upright individual having in intellect the customary support of the working framework of my computer and utilize of antivirus assurance.	0.850
I am utilized to performing exercises which guarantee my privacy and security in employing an individual computer and the Web.	0.822
I routinely overhaul (or empower a programmed upgrade) of antivirus security on my individual computer.	0.857
Cronbach Alpha	**0.945**
Eigenvalue	**6.287**
% of Variance	**69.854**
KMO=0.706; χ^2=357.777; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.4 Validity and reliability results for Perceived Privacy Risk

Three factors were utilized to analyse the concept to estimate perceived privacy risk. After meeting the Kaiser-Meyer-Olkin (.711), determinant (.006), and Bartlett's Sphericity Test (X2(3) = 616.332; p0.05) assumptions, factor analysis was performed on all three items. The three components utilized to calculate the construct's load were all significantly loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. The Cronbach's Alpha value was.833. This implies that the three factors correctly measured the variable, perceived privacy risk. To assess the concept, perceived privacy risk, the naive technique was utilized.

Table 6: Exploratory Factor Analysis on Perceived privacy risk

	Factor Loading

Shopping online is unsafe.	0.878
Giving credit card data online is unsafe.	0.927
Giving individual data (i.e., social security number and mother's lady title) online is hazardous.	0.873
Cronbach Alpha	**.833**
Eigenvalue	**3.502**
% of Variance	**50.030**
KMO=0.711; χ^2=616.332; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.5 Validity and reliability results for Customer Intrinsic Characteristics

Three components were employed to gauge consumer intrinsic attributes when evaluating the concept. After meeting the Kaiser-Meyer-Olkin (.724), determinant (.011), and Bartlett's Sphericity Test (X2(3) = 494.554; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.931. This implies that the three factors correctly measured the variable, customer inherent attributes. To measure the construct, customer intrinsic qualities, the naive technique was applied.

Table 7: Exploratory Factor Analysis on customer intrinsic characteristics

	Factor Loading
Shopping on the web permits me to spare cash.	0.892
Shopping on the web permits me to spare time.	0.877

Shopping on the Web gives me get to a wide assortment of items and administrations.	0.856
Cronbach Alpha	**.931**
Eigenvalue	**6.238**
% of Variance	**62.385**
KMO=0.724; χ^2=494.554; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.6 Validity and reliability results for Situation Factors

Three elements were employed to quantify scenario aspects when evaluating the concept. After meeting the Kaiser-Meyer-Olkin (.689), determinant (.013), and Bartlett's Sphericity Test (X2(3) = 463.253; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. The Cronbach's Alpha value was.889. This implies that the three parts accurately measured the changeable, situational aspects. To assess the concept, scenario factors, the naive technique was utilized.

Table 8: Exploratory Factor Analysis on situation factors

	Factor Loading
I buy things online based on my current area.	0.830
I exchange online due to the accessibility of my needs on the online app.	0.906
The buys I do online is based on the wild outfitted burglary cases recorded.	0.853
Cronbach Alpha	**.889**
Eigenvalue	**2.238**
% of Variance	**74.594**

KMO=0.689; χ^2=463.253; df=3; p-value=0.000

Source: Author's Field Survey (2022)

5.1.2.7 Validity and reliability results for Website Characteristics

Three criteria were employed to quantify website attributes while evaluating the construct. After meeting the Kaiser-Meyer-Olkin (.762), determinant (.003), and Bartlett's Sphericity Test (X2(3) = 838.199; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was.719 at the time. This implies that the three parts correctly measured the variable, website attributes. To assess the concept, website attributes, the naive technique was utilized.

Table 9: Exploratory Factor Analysis on website characteristics

	Factor Loading
I learned effectively to shop on the Web due to the neighbourliness of the websites.	0.927
Shopping on the web is for me a clear and reasonable prepare.	0.866
I gotten to be effortlessly skilful at shopping on the Web.	0.911
Cronbach Alpha	**.719**
Eigenvalue	**2.578**
% of Variance	**85.934**
KMO=0.762; χ^2=838.199; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.8 Validity and reliability results for Customer and Web site relationship

Three factors were employed to measure the website relationship variable while evaluating the construct. After meeting the Kaiser-Meyer-Olkin (.849), determinant (.10), and Bartlett's

Sphericity Test (X2(3) = 430.651; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.863. This implies that the three parts accurately measured the variable, customer, and website relationship. To assess the construct, website relationship variable, the naive technique was applied.

Table 10: Exploratory Factor Analysis on website relationship variable

	Factor Loading
Losing data security through social systems would posture genuine issues for me.	0.921
Online personality robbery through social systems would make genuine issues for me.	0.953
Abuse of individual data accessible in social systems would posture genuine issues for me.	0.889
Cronbach Alpha	**.863**
Eigenvalue	**2.826**
% of Variance	**60.877**
KMO=0.849; χ^2=430.651; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.9 Validity and reliability results for Legislation and Government Privacy Protection

Three factors were utilized to evaluate the design to gauge legislation and government privacy protection. After meeting the Kaiser-Meyer-Olkin (.672), determinant (.530), and Bartlett's Sphericity Test (X2(3) = 246.079; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5).

Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.790. This implies that the three factors, law, and government privacy protection, were accurate in measuring the variable. To assess the build, regulation, and government privacy protection, the naive technique was utilized.

Table 11: Exploratory Factor Analysis on legislation and government privacy protection

	Factor Loading
I know there are compelling laws to ensure customer's protection counting those relating to online exchange	0.823
I know there are compelling laws to combat cybercrime	0.761
I know the lawful environment is conducive to conduct my online exchange exchanges	0.831
Cronbach Alpha	**.790**
Eigenvalue	**2.947**
% of Variance	**64.893**
KMO=0.672; χ^2=246.079; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.10 Validity and reliability results for short term transaction

Three components were employed to examine the construct to measure short-term transaction. After meeting the Kaiser-Meyer-Olkin (.687), determinant (.849), and Bartlett's Sphericity Test (X2(3) = 263.499; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.781. This implies that the three parts correctly measured the variable, short-

term transaction. To measure the construct, short term transaction, the naive technique was applied.

Table 12: Exploratory Factor Analysis on short term transaction

	Factor Loading
I feel certain that these websites' protection articulations reflect their commitments to secure my individual data.	0.821
With their protection articulations, I accept that my individual data will be kept private and private by these websites.	0.823
I accept that these websites' protection explanations are a viable way to illustrate their commitments to protection.	0.749
Cronbach Alpha	**.781**
Eigenvalue	**2.381**
% of Variance	**64.049**
KMO=0.687; χ^2=263.499; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.11 Validity and reliability results for Established Relationship

Three factors were employed to examine the construct to measure the established link. After meeting the Kaiser-Meyer-Olkin (.546), determinant (.556), and Bartlett's Sphericity Test (X2(3) = 227.491; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.761. This implies that the three parts correctly measured the variable, formed association. To measure the construct, formed connection, the naive technique was utilized.

Table 13: Exploratory Factor Analysis on established relationship

	Factor Loading
I tend to visit to some degree "untrustworthy" web pages on which malevolent programs may well be found.	0.815
I think that no individual will endeavour an unauthorized get to my post box, and indeed in case they attempted, they might not succeed.	0.884
I once in a while take any degree for assurance of my protection when using the Web since I accept that there's no extraordinary reason for security infringement to happen to me actually.	0.687
Cronbach Alpha	**.781**
Eigenvalue	**2.381**
% of Variance	**64.049**
KMO=0.687; χ^2=263.499; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.2.12 Validity and reliability results for Privacy and Security Online

Three components were utilized to examine the concept to measure online privacy and security. After meeting the Kaiser-Meyer-Olkin (.707), determinant (.273), and Bartlett's Sphericity Test (X2(3) = 502.916; p0.05) assumptions, factor analysis was performed on all three items. The construct's three measuring components were all substantially loaded (>.5). Reliability tests were performed on the three (3) items using the Cronbach Alpha. Cronbach's Alpha was calculated to be.732. This implies that the three aspects were accurate in assessing the variable, privacy, and internet security. The naive technique was used to assess the internet concept, privacy, and security.

Table 14: Exploratory Factor Analysis on privacy and security online

	Factor Loading
In case I utilize my credit card to buy something on social media, I am stressed that as well much cash will be charged from my card.	0.858
I'm stressed that a message I post on social media can be examined by somebody else other than the individual I'm sending it to.	0.908
I am stressed that a message I post on social media could be misshaped and sent to others.	0.856
Cronbach Alpha	**.732**
Eigenvalue	**2.292**
% of Variance	**76.398**
KMO=0.707; χ^2=502.916; df=3; p-value=0.000	

Source: Author's Field Survey (2022)

5.1.3 Model One Analysis

The first model examined online privacy and security as a function of cultural variables, institutional factors, demographic factors, and online privacy and security. The model results are shown in the tables below.

5.1.3.1 Diagnostic Tests

To draw conclusions regarding the relationships between the research variables, a diagnostic test was performed. The tests were done to determine whether an empirical study of the data using multiple regression analysis was required. When the basic assumptions are met, as Greene (2002) illustrates, regression may be calculated correctly. Therefore, multicollinearity and autocorrelation among the research variables were discovered. To test for collinearity, the

variance inflation factor (VIF) was utilized, whereas the Durbin Watson test was used to test for independence.

5.1.3.2 Test of Multicollinearity

In the study, the variance inflation factor was utilized to test for multicollinearity (VIF). According to Field (2009) and Landau and Everitt (2004), VIF values less than 10 and tolerance values more than 0.2 rule out the possibility of multicollinearity among the study variables. The outcomes of the multicollinearity experiment are summarized in Table 17. According to Field (2009) and Landau et al., the VIF values for the predictor variables were less than 5, suggesting that there was no possibility of multicollinearity among the study variables (2004). The findings show that all the variables passed the test and that there was no indication of multicollinearity. Therefore, because the variables are unrelated, regression may be utilized.

5.1.3.3 Test of Independence

The auto correlation test, also known as the independence of error, terms, denotes the independence of observations. The Durbin Watson (DW) test was used to ensure that the model's residuals were not autocorrelated. According to Garson (2012), DW values ranging from 0 to 4 and scores between 1.5 and 2.5 indicate independent observations. Table 15 demonstrates that the empirical model's residuals are not autocorrelated, with D.W = 1.941 ranging between 1.5 and 2.5, meaning that all variables exceeded the required threshold of less than 2.5 and that no auto correlation was observed, as stipulated by Garson (2012).

5.1.3.4 Goodness of Fit

Table 15 exhibited the summary findings of the model, which were calculated to indicate the explained differences between cultural variables, institutional factors, demographic factors, and perceived privacy risks on privacy and security online via R2 change. Table 15 of the model summary displays the regression findings. In the regression analysis in Table 15, the adjusted coefficient of multiple determinants = 0.889, implying that cultural variables,

institutional factors, demographic factors, and perceived privacy risk explained 88.9 percent of the variation in online privacy and security.

Table 15: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.944[a]	.890	.889	.35200	1.941

a. Predictors: (Constant), PPR, CF, IF, DF

b. Dependent Variable: PaSO

5.1.3.5 Joint Significance

The ANOVA results were calculated to illustrate the model fitness by F-ratio findings between perceived privacy risk, demographic factors, institutional factors, cultural factors and privacy and security online, as shown in Table 16 The regression findings in Table 16 showed an excellent fit of the model, with a significant value of ($F(4, 389) = 781.538$, $p < 0.05$, indicating that the suggested model fit well.

Table 16: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	387.350	4	96.838	781.538	.000[b]
	Residual	47.704	385	.124		
	Total	435.054	389			

a. Dependent Variable: PaSO

b. Predictors: (Constant), PPR, CF, IF, DF

Table 17: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.091	.067		-1.369	.172		
	CF	.096	.024	.087	4.055	.000	.625	1.600
	IF	.456	.033	.431	13.988	.000	.300	3.337
	DF	.459	.040	.460	11.431	.000	.176	5.688
	PPR	.045	.027	.049	1.645	.101	.326	3.071

a. Dependent Variable: PaSO

Note: PSO – privacy and security online; CF - Cultural Factors; IF - Institutional factors; DF - Demographic Factors; PPR - Perceived Privacy Risk

Source: Author's Field Survey (2022)

From the results, it was found that cultural factors, institutional factors, and demographic characteristics were found to be positive and significant in prediction the level of privacy and security online. These variables were significant at a significancy level of 5 percent. Perceived privacy risk was insignificant in explaining privacy and security online. This means that the variables were insignificant.

5.1.4 Model Two

The second model examined online privacy and security in connection to consumer intrinsic qualities, situational circumstances, website characteristics, customer and website relationship, and law and government privacy protection. The model results are shown in the tables below.

5.1.4.1 Diagnostic Tests

To draw conclusions regarding the relationships between the research variables, a diagnostic test was performed. The tests were done to determine whether an empirical study of the data using multiple regression analysis was required. When the basic assumptions are met, as Greene (2002) illustrates, regression may be calculated correctly. Consequently, multicollinearity and autocorrelation among the research variables were discovered. To test for collinearity, the variance inflation factor (VIF) was utilized, whereas the Durbin Watson test was used to test for independence.

5.1.4.2 Test of Multicollinearity

In the study, the variance inflation factor was utilized to test for multicollinearity (VIF). According to Field (2009) and Landau and Everitt (2004), VIF values less than 10 and tolerance values more than 0.2 rule out the possibility of multicollinearity among the study variables. The outcomes of the multicollinearity research are summarized in Table 4.10. According to Field (2009) and Landau et al., the VIF values for the predictor variables were less than 5, suggesting that there was no possibility of multicollinearity among the study variables (2004). The findings show that all the variables passed the test and that there was no indication of multicollinearity. Therefore, because the variables are unrelated, regression may be utilized.

5.1.4.3 Test of Independence

The auto correlation test, also known as the independence of error, terms, denotes the independence of observations. The Durbin Watson (DW) test was used to ensure that the model's residuals were not autocorrelated. According to Garson (2012), DW values ranging from 0 to 4 and scores between 1.5 and 2.5 indicate independent observations. Table 20

demonstrates that the empirical model's residuals are not autocorrelated, with D.W = 1.777 ranging between 1.5 and 2.5, meaning that all variables exceeded the required threshold of less than 2.5 and that no auto correlation was observed, as stipulated by Garson (2012).

5.1.4.4 Goodness of Fit

Table 18 displayed the model summary findings, which were estimated to demonstrate the explained differences between customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship, legislation and government privacy protection, and online privacy and security via R2 change. Table 1 on the model summary 18 shows the regression results. The adjusted coefficient of multiple determinant = 0.555 in the regression analysis on Table 18, implying that customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship and legislation and government privacy protection explained 55.5 percent of the variance in privacy and security online.

Table 18: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.749[a]	.560	.555	.70568	1.777

a. Predictors: (Constant), LaGPP, WC, CIC, CaWSR, SF

b. Dependent Variable: PaSO

Source: Author's Field Survey (2022)

5.1.4.5 Joint Significance

As shown in Table 19, the ANOVA results were performed to highlight the model fitness by F-ratio findings between customer intrinsic features, scenario variables, website characteristics, customer and website relationship, and law and government privacy protection. The regression results in Table 19 indicated that the model fit well, with a significant value of (F (5, 389) = 97.925, p 0.05 suggesting that the recommended model fit well.

Table 19: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	243.827	5	48.765	97.925	.000[b]
	Residual	191.227	384	.498		
	Total	435.054	389			

a. Dependent Variable: PaSO

b. Predictors: (Constant), LaGPP, WC, CIC, CaWSR, SF

Table 20: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.316	.159		1.984	.048		
	CIC	.033	.051	.034	.638	.524	.412	2.428
	SF	.626	.070	.607	8.930	.000	.248	4.032
	WC	.107	.063	.116	1.703	.089	.247	4.049
	CaWSR	.008	.061	.007	.124	.901	.321	3.117

LaGPP	.071	.045	.065	1.604	.109	.708	1.412

a. Dependent Variable: PaSO

Note: PSO – privacy and security online; CIC – Customer Intrinsic Characteristics; SF – situation factors; WC - website characteristics; CaWSR – Customer and website relationship; LaGPP – Legislation and Government Privacy Protection

Source: Author's Field Survey (2022)

From the results, situation factor was the only variable significant in this model. This indicates that out of the five models designed, only situation factors had significant effect on privacy and security online. Other variables including customer intrinsic characteristics, website characteristics, customer and website relations, and legislation and government privacy protection could not affect privacy and security online.

5.1.5 Model Three

The third model was, privacy and security online as a function of control over information collection and usage of information, short term transaction and established relationship. The model results have been presented in the Tables below.

5.1.5.1 Diagnostic Tests

A diagnostic test was used to obtain findings about the correlations between the research variables. The tests were performed to assess whether an empirical investigation of the data using multiple regression analysis was necessary. When the basic assumptions are satisfied, as demonstrated by Greene (2002), regression may be calculated accurately. As a result, multicollinearity and autocorrelation were observed among the research variables. The variance inflation factor (VIF) was used to test for collinearity, and the Durbin Watson test was employed to test for independence.

5.1.5.2 Test of Multicollinearity

In the study, the variance inflation factor was utilized to test for multicollinearity (VIF). According to Field (2009) and Landau and Everitt (2004), VIF values less than 10 and tolerance values more than 0.2 rule out the possibility of multicollinearity among the study variables. The outcomes of the multicollinearity research are summarized in Table 4.10. According to Field (2009) and Landau et al., the VIF values for the predictor variables were less than 5, suggesting that there was no possibility of multicollinearity among the study variables (2004). The findings show that all the variables passed the test and that there was no indication of multicollinearity. Consequently, because the variables are unrelated, regression may be utilized.

5.1.5.3 Test of Independence

The auto correlation test, also known as the independence of error, terms, denotes the independence of observations. The Durbin Watson (DW) test was used to ensure that the model's residuals were not autocorrelated. According to Garson (2012), DW values ranging from 0 to 4 and scores between 1.5 and 2.5 indicate independent observations. Table 23 demonstrates that the empirical model's residuals are not autocorrelated, with D.W = 1.540 ranging between 1.5 and 2.5, meaning that all variables exceeded the required threshold of less than 2.5 and that no auto correlation was observed, as indicated by Garson (2012).

5.1.5.4 Goodness of Fit

Table 21 presented the model summary findings, which were estimated to highlight the explained differences between control over information collection and utilization, short term transaction and established relationship on practice and security online via R2 change. Table 21 of the model summary displays the regression findings. In the regression analysis on Table 21, the adjusted coefficient of multiple determinant = 0.501, meaning that control over information collection and utilization, short term transaction, and established relationship explained 50.1 percent of the variation in online privacy and security.

Table 21: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.711[a]	.505	.501	.74686	1.540

a. Predictors: (Constant), ER, ColCaUoI, STT

b. Dependent Variable: PaSO

5.1.5.5 Joint Significance

As shown in Table 22, the ANOVA results were performed to highlight the model fitness by F-ratio findings between control over information collection and utilization, short term transaction and established relationship, and policy and security online. The regression results in Table 22 indicated that the model fit well, with a significant value of (F (3, 389) = 131.315, p 0.05 suggesting that the recommended model fit well.

Table 22: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	219.743	3	73.248	131.315	.000[b]
	Residual	215.311	386	.558		
	Total	435.054	389			

a. Dependent Variable: PaSO

b. Predictors: (Constant), ER, ColCaUoI, STT

Table 23: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.405	.151		2.680	.008		
	ColCaUoI	.326	.048	.270	6.827	.000	.819	1.221
	STT	.196	.077	.179	2.553	.011	.262	3.815
	ER	.428	.073	.400	5.898	.000	.279	3.588

a. Dependent Variable: PaSO

Note: PSO – privacy and security online; ColCaUoI – Control over information collection and usage of information; STT – Short term transaction; ER – Established relationship

Source: Author's Field Survey (2022)

From the table, all the three independent variables had a positive significant effect on privacy and security online. That is, control over information collection and usage of information, established relationship and short-term transaction had a positive and significant effect on privacy and security online.

5.2 Results and Discussion

5.2.1 Model one

Cultural variables, institutional factors, demographic characteristics, and perceived privacy risk were regressed on privacy and security online using model one. The outcome is shown in Table 17. There was a positive and significant link between cultural characteristics and perceived privacy risk [B=0.096; t (390) = 4.055, p 0.05] in table 17. A unit rise in cultural variables

would result in a 0.096 increase in internet privacy and security. The Internet has a wide range of cultural effects. It calls for the blurring of cultural national borders, the removal of language barriers, and the dismantling of barriers between sectors of culture for instance education, science, entertainment, and art. In view of this, the culture of an individual plays a key role in predicting their stance on whether to be much concern with privacy online.

From the Table 17, institutional factors had a positive and significant effect on privacy and security online [B=0.456; t (390) = 13.988, $p < 0.05$]. A unit increase in institutional factors would lead to a 0.456 increase in privacy and security online. A significant point is that a sizable proportion of internet users presume that main business or governmental organizations will assist them in the event of an online threat. This explains why the individual privacy and security online increases as institutions improves.

The third variable on the first model was demographic factors. The demographic factor had a positive and significant effect on privacy and security online [B=0.459; t (390) = 11.431, $p < 0.05$]. A unit increase in demographic factors would cause the privacy and security to improve by 0.459. In line with an empirical survey of Internet users, certain demographic factors, such as age, education, and income level, influence Internet users' concerns about information privacy. Other variables, such as gender and Internet experience, were discovered to have no effect. The final variable on the first model was perceived privacy risk. Unfortunately, this variable had insignificant effect on privacy and security online [B=0.045; t (390) = 1.645, $p > 0.05$]. This indicates that, the irrespective of the perceived privacy risk attached to the online trading, their level of privacy and security would not be affected.

5.2.2 Model Two

From the table, customer intrinsic characteristics had insignificant effect on privacy and security online [B=0.033; t (390) = 0.638, $p > 0.05$]. The intrinsic factors are the inner motivations or drives of the customers and the extrinsic factors are the marketer generated

Internet marketing activities. This indicates that, the characteristic within the customer plays no significant role in determining privacy and security online trading.

There is a significant relationship between situation factors and privacy and security online [B=0.626; t (390) = 8.930, p < 0.05]. A unit increase in situation factors would lead to a 0.626 increase in privacy and security online. This implies that the situations at point in time would cause a customer to trade online. In view of this, situations factors have significant role on the privacy and security online issues.

From the table, website characteristics also had a positive but insignificant effect on privacy and security online [B=0.107; t (390) = 1.703, p > 0.05]. The significancy was above 10 percent. A security issue is any unmitigated chance or powerlessness in your framework that programmers can utilize to do harm to frameworks or information. This incorporates vulnerabilities within the servers and computer program interfacing your commerce to clients, as well as your commerce forms and individuals. Ordinarily, the interface of the site can call for programmers. The study's result appeared that there was no impact on protection and security online independent of the sort or frame of the characteristics of the site.

Customer and website relationship also had insignificant effect on privacy and security online [B=0.008; t (390) = 0.124, p > 0.05]. This implies that, privacy and security online issue is not influenced by the relationship that customers have with website. The damage that hackers do to trading platforms has no significant effect on the relationship that customers have with the website. In view of this, the customer and website relationship have no influence on privacy and security issues.

Finally, legislation and government privacy protection also had insignificant effect on privacy and security online [B=0.071; t (390) = 1.604, p > 0.05]. Privacy and security online would not be affected irrespective of the legislation and government privacy. This implies that, irrespective of the level of legislation and government privacy protection, the privacy and

security online would not change. Usually, traders and customers feel protected whenever they are assured of any backing of legislation in the business they undertake online. This gives them full confidence in undertaking this business. However, the results have shown that irrespective of legislation on government privacy protection. The implication of the result shows that customers rely on their personal factors rather than relying on legislations of which they have limited control over it.

5.2.3 Model Three

From the model three, control over information collection and usage of information had a positive and significant effect on privacy and security online [B= 0.326; t (390) = 6.827, $p < 0.05$]. A unit increase in control over information collection and usage of information would lead to a 0.326 increase in privacy and security online. When customers and traders realize that they have control over the information collection and usage, their level of privacy and online security increases. This explains why most customers prefer to provide information they have control on in case they are leaked. For instance, a customer would not be able to control the damage when an information on his or personal account is being leaked. In view of this, they would only be readily to share information that they can control. This explains why a unit increase in the control over information usage causes an improvement in privacy and online security.

The second variable, short term transaction showed a positive and significant effect on privacy and security online [B=0.196; t (390) = 2.553, $p < 0.05$]. A unit increase in short term transaction would lead to a 0.196 increase in privacy and security online. In other words, the shorter the transaction, the safer the customers feel. Usually, hackers would need to access to more information before they can enter a system. In view of that, individuals who sees the transaction being short and requiring a short information would be ready to give them out without considering their privacy and online security.

Finally, established relationship had a positive and significant effect on privacy and security online [B=0.428; t (390) = 5.898, $p < 0.05$]. A unit increase in established relationship would lead to a 0.428 increase in privacy and security online. Buyers and customers who have used the platform for an exceptionally long time would build trust on the platform. This would enhance the relationship they have with the platform. Building trust and relationship with the online platform would make the customer feel safe when they are providing their sensitive information. This indicates that, established relationship would enhance the privacy and online security.

5.3 Discussion

Series of models have been used in explaining the factors that influences privacy and online security. As the study considered series of factors including, cultural factors, institutional factors, demographic factors, perceived privacy risk, customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship, legislation and government privacy protection, control over information and usage of information, short term transaction and established relationships. These models were demarcated into three models based on the literature review.

The study results showed that cultural factors, institutional factors, and demographic factors had a positive and significant effect on privacy and security online. The results contradict with the findings of Skippari et al (2022) who studied on consumer perceptions of privacy and security risks for online shopping. The study attributed security on online shopping to consumer perceptions of privacy. The perception of consumers can be changed through education. However, factors such as culture, demographic factors and institutional factors cannot be changed easily. The current study attributed privacy and security online to external factors. Individuals have limited control over these factors. For instance, privacy and security online perception that aroused because of culture of the customer cannot be easily changed.

Roca, Garcia and De La Vega (2009) also studied on the importance of perceived trust, security, and privacy in online trading systems. The study found that perceived trust also had a positive and significant effect on privacy of online trading system. Tertia and Nurbasari (2022) moreover examined on the exploratory examination of components influencing online deals. Based on their investigation, they distinguished the taking after variables to be essentially affecting online deals security: visit upgrade of web substance, nearness of choice helps, arrangement of data on the firm, nearness of FAQ segment, utilize of interactive media, arrangement of person client accounts, secure modes of information transmission, arrangement to conduct offline and online money related exchanges and security explanation. These factors have contradicted with the factors attributed to online securities in this current study. The model showed that established relationship which can come because of presence of FAQ was found to have significant effect on online security. This indicates that, the current study is an extension of what Ranganathan and Gradon (2002) examined.

5.4 Economic Implications

Everyone who purchases online is concerned about internet security, but corporate leaders, not just those in the retail industry, should be as well. Companies shop online as well, and their employees frequently use the corporate credit card for commercial transactions. Online retail enterprise partners may assist a corporation in understanding what occurs when clients wheel their virtual shopping basket to the checkout lane or choose not to because they are hesitant to give their credit card information online.

The most important business concerns about online purchasing security are like consumer concerns. Many people are concerned about personal information, particularly financial information and facts about credit or debit cards, as well as financial data. Companies can follow some of the basic guidelines provided to individual online purchasers, such as keeping browsers up to date, but there are other factors to consider. Consumer behavior patterns

influenced by concerns about the security of online purchases have the potential to make or break a company's e-commerce initiatives.

According to recent Worldpay data, 24 percent of online customers worldwide will not finish the stages of an online transaction unless they are assured that their security is being maintained along the way, as Ben Rossi noted at Information Age (Kumar, Saini & Hans, 2019). These steps involve visiting the website, reviewing the product specifications, making the purchase, and obtaining a confirmation.

Although there is a frequent misunderstanding that customers do not care about security, according to the Worldpay report, at least 25% do (Towse et al., 2021). This is true in both developed and developing nations, and it is certain to grow with each major retail security event that makes headlines. Revenues fall for a variety of causes. One of the causes for the income decline is a significant drop in internet trade. Data reveal that the continual complaints from customers on internet trade have resulted in a considerable drop in income. According to studies, there is a 25% lack of confidence in internet trading (Pee, Kang, Song & Jang, 2019; Dolnicar, 2019; Zhang, Qin, Wang & Luo, 2020).

5.5 Practical Implications

Get to the Web and the capacity to move information unreservedly over borders increments the efficiency of businesses and diminishes exchange costs, subsequently making financial development and occupations. This can be giving modern openings for small and medium-sized ventures to take an interest within the worldwide economy.

Sellers must advise consumers about the need of managing passphrases, multi-factor authentication (MFA), encrypting sensitive data, and setting up firewalls to increase the security of online trade. An item of hardware or software known as a security system stands in between a computer and the internet. It controls all incoming and outgoing traffic as the

gatekeeper. The installation of a security system will safeguard the client's internal networks, but it does require routine patching to function properly.

5.6 Theoretical implications

The study also implies that external factors such as the demographic characteristics, institutional factors, and cultural factors can affect the behavior of the individual. Cultural factor can consistently create a pattern of behavior of the customer. Likewise, a demographic characteristic can also improve on the behaviour of the individual. These patterns of behaviour can cause the customer of an online trading platform to be much concern about the security and privacy. The study therefore confirms the theory of planned behavior has an implication on privacy and security online. The theory of planned behaviour explains why cultural factors, demographic factors, institutional factors, and perceived risks influences the behaviour of individual in their activities on online transactions. The behaviour of respondents is affected when they are influence by environmental and institutional factors. Moreover, the experiences on the websites can also influence the individual’s online security and privacy mentality and approach.

6.0 Conclusion

The main purpose of the study was to analyse the appropriate models for the study. Three models were deduced from the literature review. The first existing model was the relationship of cultural factors, institutional factors, demographic factors, and perceived privacy risk on privacy and security online. The result showed a coefficient of determination of 88.9 percent. This indicates that the variables explained 88.9 percent of the variations in privacy and security online. Model one happened to have the highest adjusted R-square. The second model had relationship between customer intrinsic characteristics, situation factors, website characteristics, customer and website relationship and legislation and government privacy

protection on privacy and security online. The model two recorded an adjusted R-square of 55.5 percent. The third and final model had variables such as control over information and usage of information, short term transaction and established relationships on privacy and security online. This also showed an adjusted R-square of 50.1 percent.

The study therefore concludes that, the appropriate model for privacy and security online for customers of online training is a function of cultural factors, institutional factors, demographic factors, and perceived privacy risk.

7.0 References

ABARCHI, Adamou. Leveraging Economic Development with e-Business in West African Developing Countries. International Journal of e-Education, e-Business, e-Management, and e-Learning [online]. 2013 [cit. 2022-05-18] ISSN 20103654. Available from: doi:10.7763/ijeeee.2011.v1.64

ABDELHALIM, A., and Issa TRAORE. The Impact of Google Hacking on Identity and Application Fraud. 2007 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing [online]. 2007 [cit. 2023-03-20]. ISSN edsair.

ADAMS, Michael D., Seth D. HITEFIELD, Bruce HOY, Michael C. FOWLER, and T. Charles CLANCY. Application of Cybernetics and Control Theory for a New Paradigm in Cybersecurity [online]. 2013 [cit. 2022-04-20]. Available from: https://arxiv.org/abs/1311.0257

AGARWAL, Ritu, and Jayesh PRASAD. The antecedents and consequences of user perceptions in information technology adoption. Decision Support Systems [online]. 1998, 22 (1), 15-29 [cit. 2022-05-13]. ISSN 01679236. Available from: doi:10.1016/S0167-9236(97)00006-7

AGWU, Edwin M., and Peter J. MURRAY. Empirical Study of Barriers to Electronic Commerce Adoption by Small and Medium Scale Businesses in Nigeria. International Journal of Innovation in the Digital Economy [online]. 2015, 6 (2), 1-19 [cit. 2022-05-01]. ISSN 19478305. Available from: doi:10.4018/ijide.2015040101

AHMADI DANYALI, Arezo. Factors influencing customers' change of behaviours from online banking to mobile banking in Tejarat Bank, Iran. Journal of Organizational Change Management [online]. 2018, 31 (6), 1226-1233 [cit. 2022-04-02]. ISSN 09534814. Available from: doi:10.1108/JOCM-07-2017-0269

AJZEN, Icek and Martin FISHBEIN. Understanding attitudes and predicting social behaviour / Icek Ajzen, Martin Fishbein . 1980. ISBN 0139364358.

AJZEN, Icek. The theory of planned behaviour: Reactions and reflections [online]. 2011 [cit. 2022-05-13]. ISSN edsair. Available from: doi:10.1080/08870446.2011.613995

AYOUBY, Reem, Anne-Marie CROTEAU, and Louis RAYMOND. 2013 46th Hawaii International Conference on System Sciences . 2013, 2842-2851. ISBN 9781467359337. Available from: doi:10.1109/HICSS.2013.258

AZADEGAN, Arash, and Jeffrey E. TEICH. Effective benchmarking of innovation adoptions. Benchmarking [online]. 2018, 17 (4), 472-490 [cit. 2022-06-12].

BARKLEY, David L., Deborah M. MARKLEY, and R. David LAMIE. E-Commerce as a Business Strategy: Lessons Learned from Case Studies of Rural and Small-Town Businesses [online]. 2007 [cit. 2022-06-20]. ISSN edsair. Available from: doi:10.22004/ag.econ.112895

BARNEY, Jay B. Organizational Culture: Can It Be a Source of Sustained Competitive Advantage? The Academy of Management Review [online]. 1986, 11 (3), 656-665 [cit. 2022-07-14]. ISSN 03637425.

BAUER, Hans H., Maik HAMMERSCHMIDT, and Tomas FALK. Measuring the quality of e-banking portals. International Journal of Bank Marketing [online]. 2005, 23 (2), 153-175 [cit. 2022-08-28]. ISSN 02652323. Available from: doi:10.1108/02652320510584395 ESEONU, C.I. and Egbue, O., (2021). Socio-Cultural Influences on Technology Adoption and Sustainable development, In the proceedings of the 2021 Industrial and System Engineering Research Conf. Y. Guan and H. Liao; Eds.

BELLMAN, Steven, Eric J. JOHNSON, Stephen J. KOBRIN, and Gerald LOHSE. International Differences in Information Privacy Concerns [online]. 2015 [cit. 2022-06-12].

BUENO, Salvador. Predicting Students' Behavioural Intention to Use Open-Source Software: A Combined View of the Technology Acceptance Model and Self-Determination Theory. Applied Sciences [online]. 2020, 10 (2711), 2711-2711 [cit. 2022-09-14]. ISSN 20763417. Available from: doi:10.3390/app10082711

DUFFETT, Rodney. The YouTube Marketing Communication Effect on Cognitive, Affective and Behavioural Attitudes among Generation Z Consumers. Sustainability (2071-1050) [online]. 2020, 12 (12), 5075-5075 [cit. 2022-10-08]. ISSN 20711050. Available from: doi:10.3390/su12125075

ESMAEILPOUR, R., Akbari, M., and Mojdehi, M. (2021). Surveying the factors relating to Website and Customer in creating trust to Electronic Banking, (Case Study: Refah Bank Branches in the City of Rasht), International Journal of Innovative Research in Science, Engineering and Technology, 3 (2).

EZE, U.C., Yaw, L.H., Manyeki, J.K. and Har, L.C. (2020). Factors affecting Internet banking adoption among young adults: Evidence from Malaysia, Proceedings of International Conference on Social Science and Humanity in Singapore (IPEDR) 5

FARRELL, Joseph. Efficiency and Competition between Payment Instruments. Review of Network Economics [online]. 2006, 5 [cit. 2022-09-29]. ISSN 14469022.

HAYLENCHALE, E., 2020. DETERMINANTS OF E-SERVICE DELIVERY IMPLEMENTATION IN ETHIOPIAN PUBLIC UNIVERSITIES: THE CASE OF DILLA UNIVERSITY (Doctoral dissertation).

HOSSAIN, Mohammad Alamgir, Shahriar AKTER, and Shams RAHMAN. Customer behaviour of online group buying: an investigation using the transaction cost

economics theory perspective. Electronic Markets [online]. 2022, 32 (3), 1447-1461 [cit. 2022-12-27]. ISSN 10196781. Available from: doi:10.1007/s12525-021-00479-y

KUKREJA, G., Bahl, D. and Gupta, R., 2021. The Impact of FinTech on Financial Services in India: Past, Present, and Future Trends. In Innovative Strategies for Implementing FinTech in Banking (pp. 191-200). IGI Global.

LJEVAKOVIC, Selmir, Ena KURTOVIC, Olja BOZANOVIC, Aleksandar JOKIC, Sabina BARAKOVIC, Mladen PERANOVIC and Anes MIROJEVIC. Security issues in wireless networks: An overview. 2016 XI International Symposium on Telecommunications (BIHTEL) [online]. 2016 [cit. 2022-06-22]. ISSN edsair.

MAZUR, Anna Maria, Jens TEN THIJE, Joost VREEKEN, et al. Regulatory framework on the UAM operational concepts of the ASSURED-UAM project. Aircraft Engineering [online]. 2022, 94 (9), 1491-1498 [cit. 2022-07-19]. ISSN 17488842. Available from: doi:10.1108/AEAT-01-2022-0021

MCCRACKEN, Martin, Denise CURRIE, and Jeanette HARRISON. Understanding graduate recruitment, development, and retention for the enhancement of talent management: sharpening 'the edge' of graduate talent [online]. 2015 [cit. 2022-12-09]. ISSN edsair. Available from: doi:10.1080/09585192.2015.1102159

OGUCHE, Daniel. Impact of Electronic Banking on the Profitability of Commercial Banks in Nigeria (2011-2018). The International Journal of Business [online]. 2021, 9 [cit. 2022-10-18]. ISSN 23218916. Available from: doi:10.24940/theijbm/2021/v9/i1/bm2101-053

OPOKU-MENSAH, Evans, and Dennis ASANTE. APPLICATION OF TWO-STAGE MCDM TECHNIQUES IN EVALUATING THE PERFORMANCE OF ELECTRONIC PAYMENT SYSTEMS IN GHANA. International Journal of Data

Mining [online]. 2019, 01-18 [cit. 2022-08-28]. ISSN 22309608. Available from: doi:10.5121/ijdkp.2019.930.

VANITHA, N. Behavioural Aspects Of Internet Banking Users An Empirical Study [online]. 2018 [cit. 2022-07-28]. ISSN 22489878. Available from: doi:10.5281/zenodo.1209916

YANG, Hanee. A Journey to Better Social Welfare: The relationship between cash transfer programs and stigma [online]. 2022 [cit. 2022-03-28]. ISSN editor.

Free Press.

Cashless Policy in Nigeria: Effects, Challenges and Prospects. Journal of Finance and Accounting [online]. 2020, 8 , 18-18 [cit. 2023-01-28]. ISSN 23307331.

Cheney, Julia S., (2018). Heartland Payment Systems: Lessons Learned from a Data Breach, FRB of Philadelphia - Payment Cards Centre Discussion Paper No. 10-1. Accessed 15 January 2023 from http://dx.doi.org/10.2139/ssrn.1540143.

Choi, S. and Zage, D., (2020). Addressing insider threat using “where you are” as fourth factor authentication, Accessed 7/2/2023 from http://www.cs.purdue.edu/homes/zaged/docs/iccst2020.pdf

Fu Tsang, N.K., Lai, M.T. and Law, R., 2010. Measuring e-service quality for online travel agencies. *Journal of Travel & Tourism Marketing*, *27*(3), pp.306-323.

Fukuyama, F. (1995). Trust: The Social Virtues and the Creation of Prosperity. New York,

Gerlach, D. (2018), “Special report: the web and you”, Accessed 12/03/2022 from www.computerworld.com.au/article/60937/special_report_web/

Given, L. M. (2018). *The Sage encyclopaedia of qualitative research methods*. Los Angeles, Calif.: Sage Publications. ISBN 1-4129-4163-6.

Graeff, T.R. and Harmon, S., 2002. Collecting and using personal data: consumers' awareness and concerns. *Journal of consumer marketing*.

Gromov, G. (2020). Roads and crossroads of the Internet history, Retrieved 11/05/2015 from http://history-of-internet.com/history -of-internet.pdf

Gunn L., (2021). US charges cyber-crooks over US$45 million ATM crime, Retrieved 5th November 2021 from http://atmsecurity-pro.blogspot.com/2021/05/us-charges-cyber-crooks-over-us45.html,

Hofstede G., (2019). Cultural Dimensions for International Business <http://www.geerthofstede.com/hofstede_greece.shtml>

Hofstede, G. (1983). Culture's Consequences: International Differences in Work-Related Values. Administrative Science Quarterly. Johnson Graduate School of Management, Cornell University.**28** (4): 625–629. doi:10.2307/2393017. JSTOR 2393017.

Hofstede, G. (1991). Cultures and Organizations: Software of the mind, New York: McGraw-Hill.

Hofstede, G. (March 1993). Cultures and Organizations: Software of the Mind. Administrative Science Quarterly. Johnson Graduate School of Management, Cornell University. **38** (1): 132–134.doi:10.2307/2393257. JSTOR 2393257

Hofstede, G., 2011. Dimensionalizing cultures: The Hofstede model in context. *Online readings in psychology and culture*, *2*(1), pp.2307-0919.

Hojjati, S.N. and Rabi, A.R. (2021). Effects of Iranian online behaviour on acceptance of Internet Banking, Journal of Asia Business Studies, 7 (2).

Holt, D.H. and Wigginton, K.W. (2020). *International Management*. 2nd edition. Mason, Ohio: Thomson Southwestern.

Hong, Y.H., Teh, B.H., Vidayan, G., Soh, C.H., Khan, N, and Ong, T.S. (2021). Investigating the factors influencing adoption of Internet banking in Malaysia: Adopters perspective, International Journal of Business and Management, 8 (19).

Hoyle, R.H. (1995). Structural equation modelling: Concepts, Issues, and Applications, Sage.

Ifeonu, R.O. and Ward, R. (2015). The impact of technology trust on the acceptance of mobile banking technology within Nigeria, IEEE African Journal of Computing, and ICTs, 8 (4).

Im, I., Kim, Y. and Han, H.J., (2018). The effects of perceived risk and technology type on users' acceptance of technologies, Information & Management 45 (1), pp. 1-9.

Jaeger, R. G. and Halliday, T. R., (1998). On Confirmatory versus Exploratory Research, Herpetological, 54 (suppl.)

Jain A.K. and Kumar, A., (2020). Biometric Recognition: An overview, Second Generation Biometric: The Ethical, Legal and Social Context, The International Library of Ethics, Law, and Technology 11, DOI 10, 1007/978-94-007-3892-8_3, © Springer Science + Business B.V

Jain, A. K., Ross, A. and Uludag, U., (2015). Biometric template Security: Challenges and Solutions, Proceedings of European Signal Processing Conference (EUSIPCO) (Antalya, Turkey), September 2015

Jain, A. K., S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, (2021). Biometrics: A Grand Challenge, Proceedings of International Conference on Pattern Recognition, Cambridge, UK, Aug. 2021

Jain, A., L. Hong & S. Pankanti, (2018). Biometric Identification, Communication of ACM, 43 (2)

James, A. O. (2020). The Acceptance of Online transaction by Customers in Nigeria. *World Review of Business Research, 2*(2), 6-8.

Janakiraman, S., K.V. Sai karishna Kumar, R. R. Kumar Reddy, A. Srinivasulu, R. Amirtharajan, K thenmozhi & J. B. Balaguru Rayappa, (2021). Humming Bird with Coloured Wings: A Feedback Security Approach, Info. Technology Journal, ISBN 1812-5638/DOI: 10 3923/itj.2021 © 2021 Asian Network for Scientific Information

Javidan R. & M.A. Pirbonyeh, (2018). A new Security Algorithm for Electronic Payment via Mobile Phones, 978-1-4244-8132-3/10/$26.00 ©2018 IEEE

Jayawardhena, C., and Foley, P. (2018). Changes in the banking sector: the case of internet banking in the UK. *Internet Research: Electronic Networking Applications and Policy*, 10 (1), pp. 19-30.

Jen, W., Lu, T., and Liu, P.O. (2019). An integrated analysis of technology acceptance behaviour models: comparison of three major models, MIS Review, 15 (1).

Johnson, R.B. and Onwuegbuzie, A.J. (2021) Mixed Method Research: A research paradigm whose time has come. Educational Researcher, 33(7), pp 14-26

Joreskog, K.G. and Sorbom, D. (1993). Lisrel 8: Structured equation modelling with the Simples command language, Scientific Software International.

Juwaheer, T.D., Pudaruth, S. and Ramdin, P. (2020). Factors influencing the adoption of Internet banking: a case study of commercial banks in Mauritius; World Journal of Science, Technology and Sustainable Development 9 (3)

Kalakota, R., and Winston, A.B. (1997). *Electronic Commerce: A Manager's Guide*. Addison Wesley.

Kalliny, M. and Hausman, A. (2017). The Impact of Cultural and Religious Values on Consumer's Adoption of Innovation, Academy *of Marketing Studies*, 11(1), pp.125-136.

Kambiz, H. H. and Somayeh, A., (2020). An investigation about customers perceptions of security and trust in E-payment systems among Iranian Online consumers, Journal of Basic Application, Science Research, 2(2), 1575 – 1581

Kaplan, R. S (1985). The role of empirical research in management Accounting, Working Paper 9-785-001, Division of Research, Harvard Business School, Boston, Massachusetts.

Kaplan, S., and Sawhney, M. (2018). E-Hubs: The New B2B Marketplaces, Harvard Business Review, May-June 2018, pp. 97-103

Karimzadeh, M. and Alam, D. (2020). Electronic Banking challenges in India: An empirical investigation, Interdisciplinary Journal of Contemporary Research in Business, 4 (2).

Karjaluoto, H., Mattila, M., and Pento, T. (2021). Factors underlying attitude formation towards online banking in Finland. *International Journal of Bank Marketing*, 20 (6), pp. 261-72.

Liu, C., and Arnett, K.P., 2002. An examination of privacy policies in Fortune 500 Web sites. *American Journal of Business*.

Liu, C., and Arnett, K.P., 2002. An examination of privacy policies in Fortune 500 Web sites. *American Journal of Business*.

Martinsons, M.G., 2008. Relationship-based e-commerce: theory and evidence from China. *Information Systems Journal*, *18*(4), pp.331-356.

Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A., 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), pp.65-74.

Pincus, L.B. and Johns, R., 1997. Private parts: a global analysis of privacy protection schemes and a proposed innovation for their comparative evaluation. *Journal of Business Ethics*, *16*(12), pp.1237-1260.

Risk Management for Electronic Banking and Electronic Money Activities. Payment Systems Worldwide [online]. 1998, 9 (2), 19-24 [cit. 2022-03-22]. ISSN 10517359.

Sheehan, K.B., 2002. Toward a typology of Internet users and online privacy concerns. *The information society*, *18*(1), pp.21-32.

Shin, D.H., 2010. Analysis of online social networks: a cross-national study. *Online Information Review*.

Smith, H., 1994. *The illustrated world's religions: A guide to our wisdom traditions* (p. 256). San Francisco: HarperSanFrancisco.

Trappe, W., 2015. The challenges facing physical layer security. *IEEE communications magazine*, *53*(6), pp.16-20.

Wirtz, J., Mattila, A.S. and Oo Lwin, M., 2007. How effective are loyalty reward programs in driving share of wallet? *Journal of service Research*, *9*(4), pp.327-334.

Zou, S.Y., Chen, D.J. and Ye, Y.Z., 2014. Research on fault prediction method of power electronic circuits based on particle swarm optimization RBF neural network. In *Applied Mechanics and Materials* (Vol. 687, pp. 3354-3360). Trans Tech Publications Ltd.

APPENDIX

QUESTIONNAIRE

Dear Sir/ Madam,

This intentional study may be a portion of my confirmation proposition. All the data you give here will be held with utmost confidentiality. No other individual will have rights to this data and all data will be utilized for scholastic purposes only. Please reply the taking after questions totally. It'll take around 20 minutes for you to total this study. Thank you for your time and cooperation.

1) Gender:

a. Female [ ] b. Male [ ]

2) Age (in years):

a. 25-30 [ ] b. 31-35 [ ] c. 36-40 [ ] d. 41-45 [ ] e. 46-50 [ ] f. 51- 55 [ ] g. 56-60 [ ]

3) Education (check the highest degree acquired**):**

a. [ ] Diploma b. [ ] HND c. [ ] Undergraduate Degree d. [ ] Masters (e.g. MPHIL, MBA, MSC, MA) e. [] Doctorate (e.g., PHD, DBA, DBM) f. [ ] Other professional qualification, specify…….

4. Household Income ranks a. Less than 1000 cedis b. 1001 – 5000 c. More than 5000

5) How long have you been a customer of the trading platform?

……

Instruction: Please rate the extent to which you agree with each statement.

(Please tick [✓] only one option)

From 1 = Strongly disagree to 5 = Strongly agree

	Cultural Factors	**1**	**2**	**3**	**4**	**5**
1	In my culture, there are some items one is not required to purchase online.					
2	The people who influence my behaviour believe I should not use the online transaction products and services					
3	I think customers should not question the banks' manager about the online transaction products and services.					
	Institutional Factors	**1**	**2**	**3**	**4**	**5**
1	I accept that protection seal of endorsement programs such as TRUSTe will force sanctions for online companies' noncompliance with its protection arrangement. Note: TRUSTe's Privacy Certifications provide consumer protections and applied against					

	company's online properties, data privacy and applicable regulatory.					
2	Security seal of endorsement programs such as TRUSTe will stand by me in case my individual data is abused amid and after exchanges with online companies.					
3	I am sure that protection seal of endorsement programs such as TRUSTe can address infringement of the data I given to online companies.					
	Demographic Factors	**1**	**2**	**3**	**4**	**5**
1	I consider myself as a really scrupulous individual having in intellect the customary support of the working framework of my computer and utilize of antivirus assurance.					
2	I am utilized to performing exercises which guarantee my privacy and security in employing an individual computer and the Web.					
3	I frequently upgrade (or empower a programmed overhaul) of antivirus assurance on my individual computer.					
	Perceived Privacy Risk	**1**	**2**	**3**	**4**	**5**
1	Shopping online is unsafe.					
2	Giving credit card data online is hazardous.					

3	Giving individual data (i.e., social security number and mother's lady title) online is unsafe.					
	Customer Intrinsic Characteristics	**1**	**2**	**3**	**4**	**5**
1	Shopping on the web permits me to spare cash.					
2	Shopping on the web permits me to spare time.					
3	Shopping on the Web gives me get to a wide assortment of items and administrations.					
	Situation Factors	**1**	**2**	**3**	**4**	**5**
1	I buy things online based on my current area.					
2	I exchange online due to the accessibility of my needs on the online app.					
3	The buys I do online is based on the uncontrolled equipped theft cases recorded.					
	Website Characteristics	**1**	**2**	**3**	**4**	**5**
1	I learned effortlessly to shop on the Web due to the invitingness of the websites.					
2	Shopping on the web is for me a clear and reasonable handle.					
3	I ended up effectively skilful at shopping on the Web.					
	Customer and web site relationship	**1**	**2**	**3**	**4**	**5**
1	Losing information assurance through social frameworks would pose honest to goodness issues for me.					

2	Online character burglary through social frameworks would make honest to goodness					
3	Abuse of individual data accessible in social systems would posture genuine issues for me					
	Legislation and government privacy protection	**1**	**2**	**3**	**4**	**5**
1	I know there are effective laws to protect customer's privacy including those relating to online transaction					
2	I know there are effective laws to combat cyber crime					
3	I know the legal environment is conducive to conduct my online transaction transactions					
	Control over information collection and usage of information	**1**	**2**	**3**	**4**	**5**
1	The degree of information that I feel I have in making my buy choice is adequate.					
2	The degree of control that I feel I have in making my buy choice is adequate.					
3	The degree of assets that I feel I have at my transfer in making my buy choice is adequate.					
	Short term transaction	**1**	**2**	**3**	**4**	**5**
1	I feel certain that these websites' protection explanations reflect their commitments to secure my individual data.					

2	With their protection explanations, I accept that my individual data will be kept private and secret by these websites.					
3	I accept that these websites' protection explanations are a viable way to illustrate their commitments to security.					
	Established relationship	**1**	**2**	**3**	**4**	**5**
1	I tend to visit to some degree "untrustworthy" web pages on which pernicious programs may be found.					
2	I think that no individual will endeavour an unauthorized get to my letter box, and indeed on the off chance that they attempted, they may not succeed.					
3	I once in a while take any degree for security of my security when utilizing the Web since there's no uncommon reason for security infringement to happen to me actually.					
	Privacy and Security Online	**1**	**2**	**3**	**4**	**5**
1	If I use my credit card to purchase something on social media, I am worried that too much money will be charged from my card.					
2	I am worried that a message I post on social media might be read by someone else besides the person I am sending it to.					

3	I am worried that a message I post on social media might be distorted and forwarded to others.					