IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/44ISM/2024/4445624/
Vol. 2024 (17), Article ID 4445624

Analysing Security and Privacy Issues in Electronic Payment Transactions In E-Commerce Environment: A Qualitative Research on Saudis Consumers' Behaviour In Saudi Arabia*

Haya ALSHEHRI

University of Salford, United Kingdom

Correspondence should be addressed to: Haya ALSHEHRI, h.a.alshehri1@salford.ac.uk

* Presented at the 44th IBIMA International Conference, 27-28 November 2024 Granada, Spain

Abstract

Currently, e-commerce Business-to-Consumer (B2C) is vital for companies and is very popular in Saudi Arabia, although security and privacy concerns could pose several challenges to Saudis' consumer behaviour. The current study goals to determine the actual interest of developing research investigates the impact of trust factors which are security and privacy on e-commerce payment transactions and the protection of customers' privacy of personal information. The goal of this study is to examine how Saudi consumers have changed over the last eight years in relation to trust factors as security and privacy, the study adopts a qualitative approach via semi-structured interviews to enable in-depth information from 11 interviewers to facilitate a comparative analysis with the results obtained from outcomes eight years prior, this study will incorporate a newly developed model with updated outcomes. This enhancement aims to leverage the model's capabilities to advance B2C improvements within Saudi Arabia. The findings of this study indicate that most respondents expressed a high level of trust in well-established and large companies. While concerns regarding payment security persist, respondents demonstrated a willingness to make online payments through the available payment methods. The availability of alternative online payment options, beyond traditional credit cards, such as prepayment cards, Apple Pay, and third-party payment gateways like Sallah and Zid, is viewed positively. Most participants highlighted that their primary concern in marketing is ensuring the security and privacy of their payment information. Despite these apprehensions, they recognized a notable increase in trust over the past eight years, driven by advancements in technology. Consequently, all respondents observed an improvement in trust levels since these technological developments. Nonetheless, further research is advised to address additional trust-related concerns.

Keywords: E-Commerce, Business-to-Consumer (B2C), Saudi Arabia (SA), Trust, Security, Privacy.

Introduction

E-commerce is the practising of buying and selling online, it has evidence to be a great chance to offer substantial potential for businesses to expand their customer base worldwide and increase revenue. E-commerce in Saudi Arabia is growing rapidly, driven by many factors such as government provision, increasing internet reach and smart population therefore, potentially reaching USD 27.37 billion by 2029 (Mordor intelligence, 2024). With this growth there are many concerns related to applying e-commerce such as security and privacy. As a result, customer rating, trustworthiness, and credit card security were investigated customers' security outlook concerning several leading mobile commerce applications in (SA). Customers perceive that mobile commerce applications in Saudi Arabia requires additional development in security (Gull et al. 2022). Alkhalil et al. (2024) said customer privacy was significantly underlined the impact on customer trust and the ease of decision-making

Cite this Article as: Haya ALSHEHRI Vol. 2024 (17) "Analysing Security and Privacy Issues in Electronic Payment Transactions In E-Commerce Environment: A Qualitative Research on Saudis Consumers' Behaviour In Saudi Arabia " Communications of International Proceedings, Vol. 2024 (17), Article ID 4445624, https://doi.org/10.5171/2024.4445624

in online transactions. Saudi has one of the highest percentages of internet usage in the area, among about 91% of Saudis do their shopping online, the availability of high internet penetration has drastically advanced the growth of e-commerce (Setupinsaudi, 2024). As e-commerce continues to grow, increasing fears of cyber threats underscore the necessity for businesses to implement robust cybersecurity measures to protect consumer data from potential breaches (NCA, 2024). Despite its significant growth potential, the e-commerce sector faces numerous challenges. Among the foremost concerns are issues of trust, as many customers remain apprehensive about fraud and security, leading to hesitance in engaging in online shopping. Additionally, logistical hurdles, particularly the rising costs associated with geographical expansion, pose substantial challenges (Setupinsaudi, 2024). However, technological advancements and increased internet penetration have contributed to substantial growth in e-commerce within (SA). By Saudi Arabia's e-commerce Law, companies can only keep personal information required to complete transactions, it cannot be held for further use without customer consent (kadasa, 2024) "Personal Data Protection Law (PDPL)" 2021, establishes a comprehensive framework for data privacy applicable to all personal data processed within the Kingdom. This legislation emphasizes the necessity of adopting robust security measures to safeguard personal data against unauthorized access and misuse, regardless of the nationality of the individual affected (Creationbc, 2024). Privacy concerns significantly hinder the adoption of e-commerce, often shaped by cultural perspectives within a society (Akour et al., 2022). For instance, many Saudi online customers express apprehension regarding safety and security. Additionally, research indicates a correlation between e-commerce usage and the security and privacy concerns held by both Saudi customers and merchants (Alharbi et al., 2021). In light of this progress, the need for robust data privacy regulations has become crucial to safeguard customers' personal information during online transactions (kadasa, 2024). Despite all these concerns, customers are continuing to buy more via the Internet due to the spread of applications as well as the development and support of e-commerce in Saudi Arabia, with customers believe to do their shopping online.

Aims & Objectives

This research study aims to enhance the understanding of how trust factors in business-to-consumer (B2C) e-commerce transactions and the protection of customers' personal information influence the attitudes of Saudi customers towards online shopping. To accomplish this, the subsequent three goals are developed as follow:

1) To establish whether any difference in attitude towards e-commerce is evident among Saudis nationals in the current development in e-commerce environment.
2) To explore the factors that might affect Saudis in their decision to engage with e-commerce in the current situation.
3) To explore the changes in the past 8 years in the trust aspects factors, security and privacy, that might affect Saudis in their decision to engage with e-commerce without any hesitation. (Alshehri, 2023: p. 275).

The remaining of the paper is organized as follows. In section 2, a background of e-commerce and trust of security and privacy, payment transactions, section 3 providing the research methodology and section 4 analysing the outcomes of the study, and section 5 summarizes the study.

Literature Review

The swift integration of e-commerce technologies has fundamentally altered trade practices, establishing itself as a vital component of modern economies (Binsaif, 2022). Key factors such as trust and perceived credibility significantly shape consumers' intentions to make online purchases, which are crucial for overall satisfaction in e-commerce (Attar et al., 2021). As internet transactions become more prevalent, consumer loyalty is increasingly linked to the reliance on technology. Saudi Arabia is positioning itself as a prominent market within the global e-commerce sector, currently ranked 28th, with expected revenues reaching approximately US$10,041.7 million by the end of 2023. This figure is anticipated to grow to around US$16,660.0 million by 2027 (ECBD, 2023). The country's recent budget allocation of SAR 1,114 billion in 2023 underscores a significant investment in digital initiatives. Despite the growth trajectory of the e-commerce marketplace in (SA), which recorded B2C spending exceeding SAR 29.7 billion in 2016 (Citc.sa, 2017), security concerns still pose challenges. In the eCommerce Marketplace, expected users will be 19.3m users by 2029 and user penetration will be expected to hit 49.4% by 2029 (Statista.com, 2024). To lessen possible risks associated with online transactions, service providers need to establish robust security frameworks for mobile payment solutions (Almaiah et al., 2022). The relationship between trust and security plays a critical role in shaping consumers' perceived trust, surrounding essential elements such as reputation, privacy, and data protection (Alqahtani & Albahar, 2022).

An effective framework for information security, particularly concerning computer security, data security, and online transactions within e-commerce applications, is essential. The security of transactions in e-commerce applications relies on several critical factors, including integrity, confidentiality, non-repudiation, and privacy, among others, to ensure secure and scalable operations. Therefore, a variety of security methods are developed to ensure the security of online transactions in applications based on e-commerce (Husain and Haroon, 2020). Therefore, people won't hesitate to utilise the e-commerce platform if the online payment system is straightforward, safe, easy to use, and highly secured. Hence, there are aim consideration required by players in an online transaction are the online seller, e-commerce page, and payer's perception (El Haddad, et al. 2018). Customers' apprehensions regarding credit card usage, information security, motivational strategies employed by businesses to encourage shopping, and individuals' evaluations of the reputation of e-commerce entities significantly influence their views of online data security and their overall trust in e-commerce applications (Saeed, 2023).

For businesses, understanding the consumer base's apprehensions regarding the security and privacy of e-commerce applications is essential for creating effective regulatory measures and secure technological infrastructures (Saeed, 2023). Interestingly, Saudis residing in the UK exhibit a higher degree of confidence in online transactions compared to those in Saudi Arabia, showing a greater readiness to provide their payment information (Alshehri & Meziane, 2017).

There are two types of privacy concerns among clients: the unauthorized reuse of personal data for unrelated purposes, including sharing with third parties, and the risk of unauthorised access due to security breaches or inadequate internal controls (Gupta and Dubey, 2016). Consumers express apprehension regarding the unauthorized reuse of their data for reasons impertinent to their consent, particularly concerning distributing with third parties. Furthermore, there are significant concerns about illicit access to personal information resulting from security breaches. Transactional security in e-commerce ensures the safe and legitimate transfer of funds from payer to recipient through digital means, linking the transaction data to actual economic value. A primary concern for customers is safeguarding payment card details throughout this process. Therefore, transparency in transactions is essential: financial information should not be retained once a transaction is completed, and measures must be in place to prevent this data from being shared or sold to external parties (Hussain, 2013). Online transactions entail a significant amount of private information disclosure from clients to vendors, hence increasing the danger of confidential and sensitive information leakage.

An increased awareness of security measures could bolster the effectiveness of e-commerce platforms (Qasaimeh et al., 2022). However, there is still a gap in understanding the reasons behind the slower believe of Saudis with e-commerce trust in security and privacy, necessitating further investigation into consumer behaviour and the effects of a developed e-commerce environment on their purchasing patterns.

Research Methodology

A deductive approach was chosen as shown in Figure 1, a qualitative method was adopted in this study which allows to gain an in-depth information and understanding of the matter's phenomena. It is conducted for exploration purpose approach based on qualitative findings for further information purpose (Alamer,2022). Qualitative research approach search for obtaining depth information via interviews and observation which cannot be extracted by numbers, "Qualitative research is an umbrella term for an array of attitudes towards and strategies for conducting inquiry that are aimed at discovering how human beings understand, experience, interpret, and produce the social world". (Sandelowski 2004: 893). As the nature of qualitative study is iterative and expanding, interim innovations could be applied to inform continuing data collection analysis. A semi-structured interview was designed, and interview questions, answers and discussions were all in Arabic, which the researcher translated into English. The interviews were conducted remotely. This study is focused on Saudi's who buy online; this study was conducted with 11 Saudi applicants between the ages of 20-45 years old including 4 male and 7 female participants, the participant pool for this study was drawn from a previous research project (Alshehri, 2015), with individuals who had agreed to participate in the current study. The sample included both male and female participants from various professional backgrounds, including computer administrators, project managers, social analysts, and entrepreneurs. Additionally, the female participants held positions such as banker, entrepreneur, housewife, marketing specialist, two teachers, and a manager. The total number of participants, which included seven females, was considered sufficient to fulfil the objectives of this study. Regarding educational qualifications, six males and six females held bachelor's degrees, while one female participant held a master's degree. Interviews were conducted between the end of July and September 2024. This participant pool was considered adequate for the study's requirements. A qualitative content analysis was applied to classify the impact of trust factors in the payment transaction environment on the behaviour of customers' decision to procurement

online in (SA). In this study, qualitative findings were used to obtain more information about the relative strengths of these issues, the key questions focus on gaining an understanding of the phenomenon under investigation. The interviews were conducted from Saudi nationals living in SA who have agreed to provide data from the original research (Alshehri, 2015). The interview questions from (1-9) obtained from the previous study (Alshehri, 2015), whereas question (10, 11, 12,13) obtained from the previous study (Alshehri, 2023). This project studies the impact of trust factors in B2C e-commerce transactions and highlights the influence of the environment on Saudi consumers' behaviour regarding trust in security issues on the online payment systems.

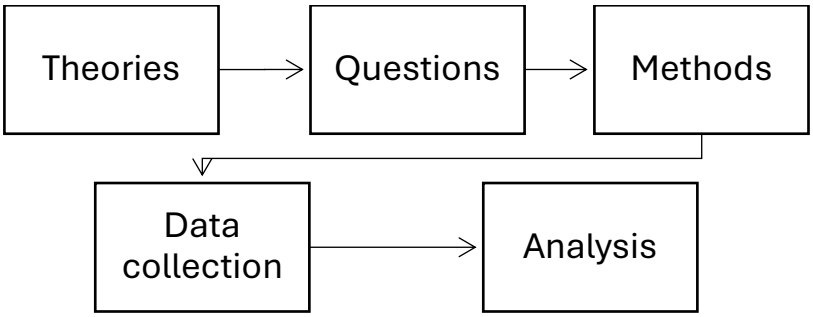

Figure 1: Deductive approach

Results And Analysis

The analysis of qualitative data derived from interviews with 11 customers reveals insights into consumer beliefs and trust dynamics regarding security and privacy in an e-commerce Environment on Saudis Consumers' Behaviour in Saudi Arabia**.** The interviews discovered that though most of candidates have high understanding of trust in security and privacy issues concern on the online payment systems. All applicants showed a clear knowledge of trust in security and privacy in online shopping and all of them have bought and paid online via different methods, they have positive impression of understanding the advantages of buying online such as saving time, effort, and access big numbers of companies online therefore, thus making payments online. The following part are the results and analysis for all questions that were answered by the participants *via* the interviews, and that will be looking at questions from Q1 to Q13.

Question 1: Do you mind providing your payment details to local companies?

Participants expressed mixed views on sharing payment details with local companies, with trust often linked to the company's reputation, registration status, and past experiences with security. Many participants were comfortable sharing payment information with well-known companies, especially those with established reputations. For instance, one participant shared, *"If the company is reliable or well-known, like Saudi Airlines, I'll provide my payment details."* Similarly, another emphasized trust in registered businesses, noting, *"If it's registered with the Ministry of Commerce, I trust it."* For smaller or lesser-known companies, however, several participants preferred using third-party services like Tamara or Zid. One explained, *"If the company is unknown, I use a prepaid card or third-party payment service."* Some participants also opted for extra precautions, such as prepaid cards or Apple Pay, when dealing with smaller vendors. One participant, who had previously faced security issues, shared, *"I only trust Apple Pay now and verify the company first."* Overall, while participants were generally open to sharing payment details with reputable companies, many opted for additional security measures when dealing with unfamiliar ones.

Question 2: Do you mind providing your payment details to overseas companies?

Participants displayed varying levels of trust when it came to sharing payment details with overseas companies, with trust primarily shaped by the company's reputation and their past experiences. Many participants were comfortable sharing payment details with well-established, reputable companies. One participant remarked, "If it is reliable and well-known, like Booking.com, I will provide my payment information. Otherwise, I avoid it." Another stated, "I don't mind sharing details with companies like Amazon or iHerb, but if I don't know the company, I won't buy."

For some, trust also depended on the availability of secure third-party payment options. As one participant explained, "If the company is large with a known brand, I trust it. For unknown companies, I prefer to use a prepaid card or a trusted third-party payment service, like Sallah or Zid." Additional precautions were common when purchasing from international companies. One participant shared, "I use a prepaid Visa for all foreign purchases to avoid any potential payment or hacking issues." Another participant, who had previously lost money through a hacked website, said, "I only use Apple Pay now and only after researching the company." Overall, participants preferred sharing payment information with globally recognized companies, often opting for extra security measures like prepaid cards or trusted payment services when dealing with lesser-known or international sources.

Question 3: Do you prefer companies that provide different payment methods?

Participants generally preferred companies that offer multiple payment options, citing convenience and flexibility as major benefits. Several participants expressed a preference for options like Apple Pay, which they found especially convenient for not requiring repeated input of payment information. One participant shared, *"It provides multiple and convenient options. Sometimes I prefer Apple Pay because I don't need to add my information every time I buy online."* Another participant agreed, noting that having options allowed them to choose based on trust: *"Sometimes I want to provide my card information, but if I'm uncertain about the company, I'll use PayPal instead."*. Some participants viewed multiple payment methods as a sign of reliability, with one explaining, *"It gives an easier opportunity to pay and suggests the company is a credible option for payment."* Others appreciated the flexibility it offered depending on their situation, with one remarking, *"It's easier for me to pick what's available at the time; it's convenient."*. For local purchases, some respondents found flexibility in having the option to pay upon receipt, adding that it was more comfortable when dealing with local companies: *"It's better for flexibility and comfort, especially if there's an option to pay upon receipt."*. While most participants welcomed multiple options, a few were more cautious due to previous negative experiences with online security. One participant shared, *"After a bad experience with a hacked link, I now only use Apple Pay."* Another participant favoured Apple Pay as it was quick and secure, saying, *"Apple Pay is my preferred choice because it's easy and fast, especially if I use a Visa card that isn't linked to my main account."*. Participants valued the flexibility provided by multiple payment options, with many favouring secure methods like Apple Pay to enhance their comfort with online transactions.

Question 4: Do you think companies must have a secure online payment system?

Participants overwhelmingly emphasised the importance of secure online payment systems to protect personal information and maintain customer trust. Many participants felt that secure systems directly contribute to a company's reputation and customer loyalty. One participant explained, *"It maintains the company's reputation and protects customer information, which helps in gaining trust."* Another added that security measures should exclude intermediary companies, noting, *"The system must be secure without third-party intermediaries; the company should ensure high security."*. Some participants also highlighted the benefit of having guarantees for refunds and reliable third-party options. As one participant put it, *"A secure system ensures that if money is stolen, it can be refunded, either through a guarantee or by using a trusted third party like Tamara or Tabby."*. The availability of trusted third-party systems like PayPal or local options (e.g., Salla, Zid) was another factor in participants' sense of security. One participant shared, *"For well-known companies, I feel comfortable with direct payment due to their reputation. For others, I use PayPal or prepaid cards."*. Others stressed that companies, whether through proprietary or third-party payment gateways, must ensure high-security standards. One participant commented, *"They should have a secure online payment system, either their own or through a third-party gateway."*. Participants strongly agreed that a secure and transparent payment system is essential, with several citing third-party services as a valuable layer of protection.

Question 5: Do you think companies should make the security of the payments clear on their websites?

Many participants felt that clearly displaying payment security measures would enhance customer confidence. One participant shared, *"Yes, of course, this would build trust and credibility, especially with security codes linked to the national address for online purchases."* Another noted, *"It's important to see the payment security mechanisms, like digital certificates, to protect data."*. Others stressed that visible security measures help

customers feel safe during transactions. One participant explained, *"It's necessary for confidentiality, so customers feel safe paying easily."* Another added, *"I'm careful and read about the company's security before buying."*. Several participants specified that digital certificates were a key feature they looked for, as it ensured the site's credibility and allowed them to enter card information with confidence. One shared, *"Seeing a digital certificate gives me comfort; it confirms the company's reliability."*. For some, additional approvals from recognized entities added to this trust. One participant noted, *"They should display security information to gain trust, ideally with approval from bodies like the Ministry of Commerce."*. Participants agreed that transparent security measures, particularly digital certifications, play a crucial role in building trust on e-commerce websites.

Question 6: Do you think technology uses to protect online payment is very important?

The role of technology in ensuring secure and efficient online payment processes was widely acknowledged by participants. Many highlighted its importance in simplifying transactions and improving speed. As one participant pointed out, *"Yes, because payment processes are easier and faster."* Another emphasized, *"It's crucial for both speed and ease."* The necessity of robust security measures for electronic transactions was also a common theme. One participant noted, *"The transaction is electronic, and without online payment protection, there's no guarantee of security."* Another shared, *"Prepaid cards have made it easier to buy from websites and protect against theft. New technologies are constantly updated to help ensure security."* For others, the adoption of advanced technology was directly linked to protecting sensitive customer information. One explained, *"It's vital because it provides clear information about protection, which reassures customers when they enter payment details."* Participants universally agreed that technology is essential not only for making online payments more efficient but also for safeguarding the personal information of users.

Question 7: Do you mind for your payment details to be stored by the company for future transactions?

Participants shared a range of opinions about the storage of payment details by companies, with many expressing concerns about security and privacy. Several respondents voiced strong objections to having their payment information stored for future transactions, fearing potential data breaches. One participant stated, *"I object, due to fear of leaking payment information."* Similarly, another said, *"I don't want my data saved for future transactions, even if the company is secure."* For some, their willingness to allow data storage was conditional, depending on the company and the frequency of transactions. One participant mentioned, *"If I always order from a company I trust, it's fine, but if there are long gaps between orders, I prefer they delete my information."* Another noted, *"For airlines, I'd like them to save my information for future purchases, as I trust them."* There were also those who had negative experiences that made them hesitant to store personal data. One participant remarked, *"I don't want my payment information saved due to a past experience that made me distrustful of hacking."* Another added, *"I don't prefer to store my payment details because sites can have security issues or breaches that compromise information security."* Overall, while some participants were open to storing payment details with trusted companies, many expressed a preference for avoiding it due to privacy concerns and past experiences with security threats.

Question 8: Do you think it's important if companies' websites have a guidance explaining the payment method?

Participants unanimously agreed on the importance of clear guidance regarding payment methods on company websites, emphasizing how it enhances the user experience and builds customer trust. As one participant noted, *"Yes, it is very important because it simplifies the process, makes it easier, and gives the customer confidence, allowing them to feel less afraid."* Another explained, *"It's significant because if the payment method is new or complicated, an explanation helps reduce any hesitation when buying."* Several participants highlighted that guidance becomes especially crucial when dealing with more complex or unfamiliar payment processes. One respondent shared, *"Some company sites have complicated payment systems, so clear instructions make the process easier. If I find a site's payment process confusing, I use a prepaid card."* Another participant reflected on their experience with third-party payment services, saying, *"It was necessary for me to have guidance when I first used services like Tabby and Tamara. It took me time to get used to them."* For others, clear payment instructions were seen as essential to ensure a smooth and stress-free shopping experience. One participant emphasized, *"It's crucial, especially for new payment methods, so the customer doesn't get frustrated or abandon their purchase because they don't understand how to pay."* Participants agreed that providing clear instructions

and guidance on payment methods is vital for ensuring a positive customer experience, reducing confusion, and encouraging repeat business.

Question 9: Do you think you will buy online or buy more if your bank guarantees your transactions to be safe?

The participants largely agreed on the positive impact of bank guarantees for safe transactions on their online purchasing behaviour, with many expressing increased confidence in making purchases online when they know that their transactions are protected. As one participant put it, *"The bank often verifies suspicious transactions and contacts the customer, which gives me peace of mind."* Another participant added, *"I feel safe knowing that the bank will compensate me for any losses."* For several participants, the assurance of reimbursement in case of issues made online shopping more comfortable. *"I know that the bank will return the money if there's an issue, so I can shop without fear,"* said one respondent. Others cited services like PayPal, which offer guarantees for secure transactions, with one noting, *"PayPal ensures your money is returned if there's a problem with the site, which builds trust."* The reassurance provided by banks and payment systems led to increased willingness to make purchases. *"I feel secure and more likely to buy more when I know my transactions are protected,"* shared another participant. However, one participant remained neutral, stating, *"It depends on my needs; I don't think guarantees will significantly change my purchasing habits."*

Question 10: Do you have concerns about your bank details when you buy online and to what extend?

Participants expressed varying levels of concern about sharing their bank details when shopping online, with the extent of their anxiety influenced by factors such as the company's reliability and personal experiences. Many participants mentioned using prepaid cards or PayPal to reduce anxiety, stating, *"The extent of concern depends on the reliability of the company."* Some participants shared specific past experiences that increased their concerns. For example, one participant recalled purchasing perfume from an unreliable site, saying, *"I bought perfume and never received it; the bank didn't refund my money because it was a hacker link."* Another participant expressed concern over the growing threat of online fraud, noting, *"An acquaintance lost 4 million riyals due to a fraudulent link."* Other participants indicated that their concern depended on the type of website. One respondent said, *"It depends on the site, and I use a prepaid card when I'm worried."* Another explained that *"If it's my first time and the amount is large, I feel anxious and prefer prepaid cards for smaller amounts."* While many participants were cautious, some felt comfortable shopping with well-known companies. One participant mentioned, *"I don't feel anxious because I buy only from well-known companies."* Participants' comfort with sharing their bank details when shopping online varied, with trust in the company and their past experiences being key factors in their level of concern. Many participants preferred using alternative payment methods like prepaid cards or PayPal to reduce anxiety and enhance security.

Question 11: Do you trust online payment systems as much as 8 years ago? (why)

Participants shared mixed perspectives on how their trust in online payment systems has evolved over the past eight years. While some respondents felt that their trust had grown due to technological advancements and increased security awareness, others cited persistent concerns about hacking and data breaches. For instance, some participants maintained a cautious stance, with one noting, *"I feel the same as before because hacking and breaches still exist, so there is ongoing anxiety."* Others shared a more positive view, crediting COVID-19 and the rise of secure digital platforms for their increased confidence in online payments. As one participant put it, *"Trust has increased, especially since COVID-19, as companies have taken greater interest in protecting data."* Several respondents felt that technology had significantly bolstered their trust. One participant explained, *"Confidence has increased with the development of technology, multiple payment options, and site improvements."* Another echoed this sentiment, saying, *"I have more confidence now because e-commerce is widespread, and companies have dedicated online departments."* For some, this trust has developed over years of experience with online shopping. A participant who had been purchasing online since 2013 remarked, *"Confidence has increased due to modern technologies, though some concerns remain."* Similarly, a few participants mentioned that they felt more secure now than eight years ago, citing advancements in defences against electronic attacks as a major factor.

Question 12: Do you think you need more awareness about the online payment system?

Participants shared differing perspectives on the need for increased awareness of online payment systems. While some expressed the importance of ongoing education to mitigate potential risks, others felt adequately informed or highlighted the need for targeted awareness, particularly for those new to online transactions. For instance, some participants indicated a preference for continuous awareness, especially when using new payment systems. As one participant noted, *"It depends on the type of system. If it's new, I need more awareness."* Another respondent emphasized the importance of regular updates due to security concerns, stating, *"Yes, continuous awareness is important because breaches happen even on secure sites."* Others expressed a general desire for more clarity on secure online practices, with one participant explaining, *"Of course, we need more awareness to understand sites, links, and companies."* Meanwhile, some respondents with experience in online shopping felt they only needed occasional updates. One participant mentioned, *"I have enough experience, but I would want guidance if new electronic payment issues arise, preferably from specialists."* A few participants felt that they were sufficiently informed, particularly if they had a background in technology. For example, one respondent noted, *"As a computer specialist, I am satisfied, though society at large still needs awareness on the risks when paying online."* Another added that awareness efforts should especially benefit beginners, explaining, "Awareness is important for those new to online shopping, as many don't have time to research these topics." While many participants agreed that more awareness could enhance security for all users, those experienced in online payments emphasized the value of targeted updates and resources for specific user groups.

Question 13: Do you think your personal information is safe when you buy online?

Participants shared mixed views on the safety of their personal information when shopping online, with trust levels often varying based on the company's reputation and perceived security practices. Some participants expressed confidence in well-known companies while maintaining caution with smaller, less established businesses. For instance, several participants noted that their comfort level depends on the company's status and familiarity. One participant explained, *"It depends on the company; with names like Amazon or iHerb, I feel safer, but I'm sceptical with smaller or unfamiliar companies."* Another echoed this sentiment, stating, *"It depends on the company's strength and reputation in safeguarding electronic payment data."* Others were more sceptical of online security in general, citing concerns over data breaches and the potential misuse of personal information. As one participant remarked, *"I hope it's safe, but I don't trust it completely due to frequent breaches. Companies may claim they protect personal information, but I don't know their internal processes."* Similarly, another participant voiced general apprehension, saying, *"There's always a certain level of risk that varies, and a feeling that cannot be ignored."* A few participants expressed outright distrust due to the potential for unexpected data breaches. One participant shared, *"I don't believe it's secure because hackers can breach sites at any time."* Another added, "Security isn't absolute—it depends on the company's efforts, but there's always some level of doubt." While some participants felt reassured by the reputation of major companies, a pervasive sense of caution and scepticism remained, especially regarding less established businesses and the general security of online shopping platforms.

Conclusion

This paper investigates the role of trust factors in influencing perceptions of security and privacy within business-to-consumer (B2C) e-commerce transactions, specifically focusing on Saudi customers' attitudes towards online shopping. To achieve this, the study utilised interviews to collect customer insights on these critical issues. The findings highlight how trust factors impact the willingness of Saudi consumers to engage in online purchases. Furthermore, the research underscores the importance of protecting customers' personal information, which is essential for fostering trust and confidence in e-commerce. The study shows that trust factors significantly influence B2C e-commerce transactions among Saudi customers, encouraging them to make online purchases. Most participants expressed a strong level of trust in well-known and large companies, demonstrating a willingness to pay online through various payment methods. Even when they had doubts about payment security, they felt comfortable using options such as Apple Pay, prepaid cards, and third-party payment gateways like Sallah and Zid and they buy online as they are like this way of shopping nowadays. However, participants voiced concerns about the security and privacy of their information, particularly when dealing with smaller companies or those not registered on the Maroof Platform.

Additionally, the presence of government support and supervision, along with competitive pricing, emerged as critical factors in building consumer trust. The Maroof Platform, which is an electronic initiative by the Ministry of Commerce aimed at enhancing the credibility of online stores and facilitating communication with merchants, was frequently mentioned by participants. Overall, the study reveals that trust levels among consumers have

increased over the past seven years, largely due to significant technological advancements. Nevertheless, further research is necessary to explore additional trust-related issues in the context of e-commerce.

References

- Alamer, A. (2022). An empirical study of mobile commerce and customers security perception in Saudi Arabia. Electronics, 11(3), 293.
- Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., & Aldhyani, T. H. (2022). Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in SaudiArabia. Electronics, *11*(23), 3926.
- Alqahtani, M., & Albahar, M. A. (2022). The Impact of Security and Payment Method On Consumers' Perception of Marketplace in Saudi Arabia. *International Journal of Advanced Computer Science and Applications*, *13*(5).
- Alshehri, H. (2023), The Impact of Trust Factors in an E-Commerce Transactions (Security and Privacy) Environment on Saudis Consumers' Behaviour in Saudi Arabia.
- International Business information Management Association (42nd IBIMA) ISSN: 2767-9640, (p.275)
- Alshehri, H. A. D. (2015). *A framework for the implementation of B2C e-commerce in Saudi Arabia: A comparative study of Saudis living in Saudi Arabia and those living in the UK, and the perception of Saudi companies*. University of Salford (United Kingdom).
- Alshehri, H., & Meziane, F. (2017, December). The influence of advanced and secure e-commerce environments on customers behaviour: The case of Saudis in the UK. In *Internet Technology and Secured Transactions (ICITST), 2017 12th International Conference for* (pp. 332-337). IEEE.
- Alshehri, H. A. D. (2015). *A framework for the implementation of B2C e-commerce in Saudi Arabia: A comparative study of Saudis living in Saudi Arabia and those living in the UK, and the perception of Saudi companies*. University of Salford (United Kingdom).
- Attar, R. W., Shanmugam, M., & Hajli, N. (2021). Investigating the antecedents of e-commerce satisfaction in social commerce context. *British Food Journal*, *123*(3), 849-868.
- Alkhalil, B. F., Zhuang, Y., Mursi, K. T., & Aseeri, A. O. (2024, May). Game-Theory-Based Analysis of Key Factors Influencing Saudi Consumer Trust in E-commerce. In *2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-7). IEEE.
- Alharbi, A. S., Halikias, G., Rajarajan, M., & Yamin, M. (2021). A review of effectiveness of Saudi E-government data security management. *International Journal of Information Technology*, *13*, 573-579.
- Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A conceptual model for investigating the effect of privacy concerns on E-commerce adoption: a study on United Arab Emirates consumers. *Electronics*, *11*(22), 3648.
- Creationbc, (2024). *Highlights Of the E-Commerce Law in Saudi Arabia.* https://www.creationbc.com/en-sa/corporate-laws-and-legislation/e-commerce-law/ last access 25/10/2024.
- Ecommercedb (ECBD), (2023), eCommerce revenue development in Saudi Arabia, https://ecommercedb.com/markets/sa/all, Last access 27/10/2023.
- CITC (Communications and Information Technology Commission), (2017). ICT Report, E-Commerce in Saudi Arabia. P.O. Box 75606 Riyadh 11588 Saudi Arabia, http://ictreport.sa/ecommerce/References.htm, last accesed 30-09-2018.
- El Haddad, G., Aimeur, E., & Hage, H. (2018). Understanding trust, privacy and financial fears in online payment. In *2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 28-36). IEEE.
- Gupta, M. P., & Dubey, A. (2016). E-commerce-study of privacy, trust and security from consumer's perspective. *International Journal of Computer Science and Mobile Computing*, *5*(6), 224-232.
- Gull, H., Saeed, S., Iqbal, S. Z., Bamarouf, Y. A., Alqahtani, M. A., Alabbad, D. A., ... & Alamer, A. (2022). An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics*, *11*(3), 293.
- Qasaimeh, M., Halemah, N. A., Rawashdeh, R., Al-Qassas, R. S., & Qusef, A. (2022, July). Systematic Review of E-commerce Security Issues and Customer Satisfaction Impact. In *2022 International Conference on Engineering & MIS (ICEMIS)* (pp. 1-8). IEEE.
- Hussain, M. A. (2013). A study of information security in e-commerce applications. *International Journal of Computer Engineering Science (IJCES)*, *3*(3), 1-9.

- Husain, M. S., & Haroon, M. (2020). An enriched information security framework from various attacks in the IoT. *International Journal of Innovative Research in Computer Science & Technology*, *8*(4), 271-277.
- (kadasa, 2024), Saudi Arabian E-commerce Law. A Step towards Consumer Protection https://kadasa.com.sa/
- National Cybersecurity Authority (NCA), (2024). *Regulatory documents* https://nca.gov.sa/ar/regulatory-documents/. (nca.gov.sa).
- Sandelowski. M. (2004) 'Qualitative Research', in Lewis-Beck, M., Bryman, A., and Liao, T. (eds) Th e Sage Encyclopedia of Social Science Research Methods, Th ousand Oaks CA, Sage.
- Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1020.
- Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1020.
- Setupinsaudi. (2024,09). *E-Commerce Sector in Saudi Arabia Saudi E-Commerce: Robust Digital Infrastructure and Growing Demand.* https://www.setupinsaudi.com/ last access 27/10/2024.
- Statista.com, (2024). eCommerce -Saudi Arabia https://www.statista.com/, last access 29/10/2024.
- Mordor intelligence. (2024, Septemper). *Saudi Arabia E-Commerce Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029).* https://www.mordorintelligence.com/