applied sciences

MDPI

Article

A Customer-Centric View of E-Commerce Security and Privacy

Saqib Saeed

SAUDI ARAMCO Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa

Abstract: Business organizations have huge potential to increase their customer base by offering e-commerce services, especially in the post-pandemic era. Ensuring secure e-commerce applications plays an important role in increasing customer base. To develop appropriate policies and secure technological infrastructures, business organizations first need to establish an understanding of the reservations of their customers toward e-commerce, as well as their perception of security and privacy of e-commerce applications. In this paper, we present the results of an empirical study of e-commerce customers conducted in Pakistan to gain an insight into their mindset on using e-commerce applications. An online questionnaire was set up to collect data, which were analyzed using the partial least squares method with SmartPLS software. The empirical findings highlight that customers' concerns about credit card usage, concerns over information security, motivational factors for shopping offered by business organizations, customer trustworthiness, and user's feelings about the reputation of e-commerce impact their perception of security of online data and trust in an e-commerce application. The results of this study can help organizations in Pakistan to develop policies and improve technological infrastructures by adopting emerging technologies and digital forensics.

Keywords: user security; customer privacy; e-commerce; customer perception; empirical study

1. Introduction

E-commerce is the use of computing devices and communication platforms to conduct business online. It has proven to be an important enabler for business organizations by expanding their reach to global customers, cost-effectively and efficiently. This technological revolution is termed disruptive technology [1] as it has changed traditional business models and brought about new business approaches. This extensive digital transformation process requires changes in organizational processes, human resources, and technological infrastructure. To be successful, business organizations need to carry out a detailed analysis of their marketplace to develop an effective business strategy, which requires financial and human resources [2]. Furthermore, e-commerce adoption is also dependent on social, legal, economic, political, and technological factors [3]. The difference in technology accessibility, level of skills, security concerns, shopping behavior, purchasing power, cultural differences, and legislation also affect the acceptance of e-commerce [4]. As a result, the adoption of technological infrastructure by business organizations varies considerably across the globe.

Recently, COVID-19 has resulted in a rapid digital transformation in every sector and similarly, e-commerce has also gained enormous popularity and become a replacement for conventional brick-and-mortar stores during lockdown [5,6]. Akram et al. [7] highlighted that ease of use, trust, mobility, and customer involvement have resulted in an exponential increase in the use of mobile commerce during the pandemic. Gu et al. [8] highlighted that, due to COVID-19, customers have become more experienced with online shopping, and it has influenced their buying behavior. Guthrie et al. [9] observed that the purchase intentions of the customers regarding basic needs and other categories of products have seen a significant shift, as compared to pre-COVID-19 buying patterns. The ease of online shopping also brought significant security challenges for customers, as well as business

check for updates

Citation: Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. https://doi.org/10.3390/app13021020

Academic Editors: Christina Thorpe and Stephen O' Shaughnessy

Received: 9 November 2022
Revised: 26 December 2022
Accepted: 5 January 2023
Published: 11 January 2023

organizations. Business organizations have been taking a variety of cybersecurity measures to secure their e-commerce infrastructure; however, Shu and Liu [10] highlighted that there is a need to further explore privacy-enhancing technologies and associated strategies to better understand the security implications. Customers are an important stakeholder for e-commerce business organizations, and, if they are not confident that a certain e-commerce platform is secure, they will not indulge in a business transaction. Therefore, customers' perception regarding the security and trust in e-commerce is of paramount importance. Customer perception of security and trust is dependent on the national culture, which is built upon factors such as individualism, risk-taking behavior, and power structures [11]. Mohammed and Tejay [12] found that e-commerce acceptance, online safety perception, personal preferences, and privacy concerns are important factors for e-commerce adoption in a society. Clemons et al. [13] found that the reputation of business organizations affects the trust of customers differently across geographical regions.

Motivation

Differences in the banking system, legal framework, and user sensitivity toward security can impact the customer's perception of security and privacy. Most studies conducted to understand customer perception originate from developed countries, such as the USA, the UK, Singapore, China, and Poland. These countries have a lot more exposure to technology, and they have been blessed with a more reliable banking systems and robust legal infrastructures [14–17]. Therefore, it is scientifically interesting to explore the factors determining customer perception regarding the security of e-commerce applications in a developing economy. Consequently, we conducted an empirical study in Pakistan, a developing nation, to understand how e-commerce customers in Pakistan perceive security related to e-commerce and trust in online shopping. Positive perception can help to foster secure behavior in e-commerce usage whereas a negative perception may lead to limited usage of e-commerce by consumers. We used the protection motivation theory (PMT) as a theoretical model for our study.

PMT was developed by Rogers [18] to better understand fear and explain how people react to it. Perceived vulnerability, severity, response efficacy, self-efficacy, and response cost are the key constructs of PMT, and their joint impact helps in determining intentions to protect against such a threat [18]. Perceived vulnerability refers to the likelihood of being affected by the threat, perceived severity highlights the severity of the threat in case of impact, response efficacy refers to the usefulness of mitigation strategies, self-efficacy refers to the ability to carry out mitigation strategies, and response cost refers to the cost incurred to execute mitigation strategies. This theory has been applied in many domains to explain the behavior of people in different situations such as health risks [19–21], flooding, and typhoons [22]. Similarly, PMT has also been used in different cybersecurity contexts [23–25]. We, thus, used this theory in our work to understand the customer's perception regarding the security of e-commerce websites in Pakistan. We used perceived vulnerability, perceived severity, response efficacy, and response cost to understand the customer's perception of security and privacy in Pakistan. The contribution of our study presents empirical insights into customers' perceptions and trust in e-commerce in Pakistan. On the basis of the empirical data, we present a model to improve the trust and security perception of e-commerce among Pakistani customers.

The remainder of the paper is structured as follows: related work is discussed in Section 2 and research design is presented in Section 3; Section 4 presents the results, followed by a discussion in Section 5 and a conclusion in Section 6.

2. Related Work

Many studies have focused on the security aspects of e-commerce technological infrastructure, such as securing communication [26–28], secure payment mechanisms [29,30], and fraud protection [31,32]. There has, however, been an enhanced interest in customer perception of security and trust in e-commerce. Shah et al. [33] highlighted that buying intention of customers is dependent on trust and perceived benefits of the product, whereas the potential risk decreases customer trust. Liu and Li [34] identified that trust and social aspects influence customers while engaging in mobile commerce transactions. López Jiménez et al. [35] highlighted that the adoption of security seals on company websites results in increased sales, as well as increased web traffic. Dhende and Meshram [36] highlighted that intra-organization, inter-organization, and customer-to-organization data exchanges using advanced technological infrastructure result in security challenges. Tan [37] noticed that despite the advancements in e-commerce, a lack of trust for customers in business is a constant impediment to the adoption and realization of electronic commerce. E-commerce vendors need to develop trust because repairing the trust of customers is a very difficult and expensive activity. Zhang et al. [38] highlighted that, to repair customer trust, single relational strategies are not enough; rather, an integration of single transactional and integrative strategies should be deployed.

Turner et al. [39] highlighted that users with limited technical knowledge rely on the reputation of the websites, their interaction with the website, and third-party recommendations to keep them secure on the internet. Liebermann and Stashevsky [40] highlighted that demographic traits and behavior of use affect risks of using the internet, and they developed a detailed perceived risk map to make the users aware with potential risks. Belanger et al. [41] highlighted that customer perception of a merchant's trustworthiness is a key factor that encourages customers to indulge in online or conventional business transactions. Furthermore, security, privacy, and usability are the factors that affect shopping intention. Yenisey et al. [42] experimented with simulated e-commerce applications to determine the factors that cultivate positive feelings among customers. McDonald and Cranor [43] highlighted that investing time to read privacy policies of websites is a form of investment made by users and, in return, they should receive payments as they are revealing information. Huang et al. [44] analyzed how knowledge, impact, and severity of risk, probability of occurrence, and awareness affect information security behavior. They further discussed computer experience and potential loss affect user behavior. Beldad et al. [45] found that potential risks influence users to read online privacy statements, and that older people are more inclined to read privacy statements than younger people. Furthermore, people with low education levels and internet experience also have a higher probability of reading privacy statements as compared to users having higher education and more internet experience. Bonera [46] highlighted that intention to make an online purchase is affected by usable design, customer's perception of security, and usefulness of e-commerce websites. Chowdhury and Chowdhury [47] highlighted some other key factors that influence online shopping behavior including complex online shopping processes, lack of reliability, weak payment settlement systems, and traditional mentality of customers. Kasuma et al. [48] emphasized some motivations that lead to online shopping including convenience of placing orders online, timesaving, website design, and security. Zahrani [49] stressed that social influence, perceived usefulness ease of use, and trust significantly contribute to perceived risk and security, which ultimately affects consumer intention to use a credit card online. Alotaibi and Alshehri [50] conducted a study and found that men exhibit more secure behavior online as compared to women. McCormac et al. [51], however, argued that gender and age are not significant in information security behavior, but emotions and risk acceptance of users affect the information security behavior. Tang et al. [52] found in their research that governmental social media accounts can influence information security behavior among users.

Yazdanifard et al. [53] discussed that security and privacy concerns can result in negative e-commerce growth; thus, they conducted a literature review to document common reasons for privacy and security concerns. Jensen [54] argued that there is a need to include trust as an important component of security models to secure computer networks by developing quantitative and qualitative trust models. Saeed [55] carried out an empirical study on e-business adoption by expatriates in Saudi Arabia and highlighted that cultural differences between expatriate communities should be considered during the technical design stage to make systems more usable. Gupta and Nage [56] outlined a set of security concerns and associated techniques to minimize their impact in web-based business environments.

In addition to other benefits, digital transformation by business organizations also results in many security risks, not only for the organizations themselves but also for their customers. Mason [57] identified four core issues about personal information ownership: privacy, accuracy, property, and accessibility, which are critical for customers while engaging in business transactions online. Gull et al. [58] found that mobile commerce customers in Saudi Arabia expect more strict security mechanisms for a positive security perception of these platforms.

Khan et al. [59] discussed that blockchain can be used to enhance security in e-commerce by using smart contracts which ensure the privacy of transactions. Gouthier et al. [60] found the use of data analytics by e-commerce companies is dependent on customers' willingness to disclose personal information. They stressed the importance of transparent data management policies which prove critical for the customers to willingly share personal data. Mashatan et al. [61] investigated privacy and security concerns of customers in the adoption of crypto payments and concluded that there is an innate need to enhance customers' understanding of potential problems and security issues to increase crypto payments. Vuță et al. [62] conducted a systematic literature study and discussed that human factors are the main risk along with fear of cyber-attacks, and that artificial intelligence, blockchain, and machine learning technologies play a critical role in minimizing these risks.

Masyhuri [63] studied Amazon and e-Bay to identify essential elements to improve customer satisfaction with the e-retailing business. Alkis and Kose [64] carried out an empirical study across 29 European countries and presented their findings on customers with more protection against online privacy are more likely to make online purchases and companies providing a higher level of privacy attract more customers. Anshori et al. [65] carried out an empirical study with the users of Tokopedia application and found that security and privacy have a significant impact on the trust and perceived value of users, which in turn have a positive impact on reuse intention. Cebeci et al. [66] developed a secure protocol that was evaluated on electronic transaction 3D secure systems, and the results showed a reduction in security concerns, as well as low communication cost. Novita and Budiarti [67] carried out a study on "Shopee" application users and found that, even for satisfied customers, perceived security, trust, and privacy positively influence customer retention.

2.1. Protection Motivation Theory in Cybersecurity

More recently, protection motivation theory has been used in the cybersecurity literature to relate to how users respond to cybersecurity threats while working with information technology applications. Marett et al. [68] explored the behavior of social media users inline with the PMT and found that it explains the behavior of both types of users, those with serious security concerns and casual. Meso et al. [69] carried out an empirical study with PMT on college students to understand how knowledge gained regarding cybersecurity during lectures is applied in practice. Dang-Pham and Pittayachawan [23] used PMT in their empirical study at an Australian university to understand user intention while using their personal devices at home as compared to the university. They found differences in user behaviors toward malware avoidance within both contexts. Hanus and Wu [70] explored the impact of information security awareness on desktop security behavior and found that security awareness affects PMT constructs, perceived security, response efficacy, self-efficacy, and response cost. Verkijika [24] expanded on the PMT and included anticipated regret as a mediator among PMT constructs and intended behavior. He found that perceived security and perceived vulnerability have a positive influence on the anticipated targets. Chiu et al. [25] used PMT to examine the employees' incentive to observe organizational information security policies. Similarly, Erhart [71] used PMT constructs to explain employees' intention to comply with organizational security policies. Ganesh et al. [72] developed a game to increase user aware of mobile phone risks inline with the PMT, and they found that their game helped users to better tackle security issues while they used their mobiles. Mou et al. [73] contributed to information security discourse by showing how PMT and structural equation modeling can be used to verify different theories. These contributions highlight that PMT has been a central part in cybersecurity literature. The protection motivation theory examines how people respond to stressful situations against potential threats; on this basis, it could be forecasted and key indicators could be identified which result in changed behavior of people. Therefore, it is interesting to apply PMT in studying which factors contribute to users' perception of security and privacy, so that appropriate control systems can be designed.

2.2. E-Commerce Research in Pakistan

Within the context of e-commerce in Pakistan, several studies have been published over the years. Khan et al. [74] stated that internet legislation, poverty, and the lack of knowledge and infrastructure are all major barriers for e-commerce in Pakistan. Arshad and Zaidi [75] found that consumer behavior and organizational growth positively correlate with e-commerce in Pakistan, and that limited integration with organizational objectives and weak internal capabilities can be a major threat to Pakistani business organizations. Ghouri et al. [76] identified that privacy, security, and trust are important success factors for e-commerce adoption by Pakistani businesses. Anjum and Chai [77] found that the ease of use of cash on delivery helps in improving the security perception of e-commerce consumers in Pakistan. Tanveer [78] discussed how honesty and fulfillment are important factors for customer relationship building for e-commerce vendors in Pakistan. Saeed et al. [79] carried out a usability evaluation of e-commerce portals in Pakistan and highlighted the dire need for major improvements in user interface and experience. Agren and Barbutiu [80] reported that women face more cultural barriers in e-commerce adoption than men in Pakistan. Ahmed [81] raised the point that the design and implementation of an effective e-commerce policy can help e-commerce growth in Pakistan. Amjad et al. [82] discussed that the main entrepreneurial challenges for e-commerce in Pakistan include a change-resistant culture, poor law enforcement, and unprofessionalism of vendors. Imtiaz et al. [83] argued that e-business adoption in Pakistan is relatively slow, and that privacy, security, and trust factors are prerequisites for improved e-business services in Pakistan.

2.3. Hypothesis Formulation

Even though there have been several studies carried out on e-commerce and related issues in Pakistan, there is no empirical study that focused on Pakistani customers' security perception of e-commerce. National culture is an important factor that affects technology adoption practices; therefore, in this paper, we explore how customers in Pakistan perceive security and privacy issues relevant to e-commerce websites in Pakistan. The findings can help in better understanding the customer's security concerns and in the subsequent design of appropriate controls. The hypotheses were rooted in the previous literature where we identified demographic factors gender [H1], age [H2], and computer proficiency [H3], threat awareness [H4], threat perception [H5, H6, H7, and H8], security concerns [H9], motivational factors [H10], trustworthiness [H11], and reputation [H12] as key parameters for understanding security perception. As a result, our questionnaire features dedicated questions focusing on these aspects. Therefore, 12 hypotheses were developed for our study, which are listed in Table 1, along with the relevant literature. Some of the hypotheses comprised additional constructs, which are mentioned in the rows after the relevant hypothesis. The mapping of these constructs is provided in Table 2.

Table 1. List of hypotheses and associated constructs.

Nr.	Hypothesis	Relevant Study
H1	Gender has an impact on the customers' perception of the security of online data and trust in e-commerce applications.	[50,51]
H2	The age of the customer has an impact on the customers' perception of the security of online data and trust in e-commerce applications.	[40,51]
H3	Computer proficiency level has an impact on the customers' perception of the security of online data and trust in e-commerce applications.	[51]
H4	Customers who read privacy policy statements of e-commerce websites and review security certificates have a positive perception of the security of online data and trust in e-commerce applications.	[43]
H5	Customers who have a positive perception of the security of online data and trust in e-commerce applications are less prone to hacking attacks.	[44]
H6	Customers who read privacy policy statements of e-commerce websites and review security certificates are less prone to hacking attacks.	[45]
H7	Customers' rating of security aspects of e-commerce websites reflects the customer's perception of the security of online data and trust in an e-commerce application.	[11,39]
	Authentication of users by e-commerce websites	[26–28]
	Authentication of vendors by customers	[11]
	Fraud protection provisions	[31,32]
	Provision of secure communications by e-commerce websites	[26–28]
H8	Customers' credit card usage concerns reflect the customer's perception of the security of online data and trust in an e-commerce application.	[49]
	Network security issues	[46,49]
	Operating systems' security issues	[46,49]
	Applications' security issues	[49]
	Unauthorized transaction issues	[29,30]
	Fraudulent transaction issues	[29,30]
	Disputed vendors	[33]
	Product quality issues	[33]
H9	Customers' e-commerce usage concerns reflect the customer's perception of the security of online data and trust in an e-commerce application.	[40,46]
	Concerns over private information provision	[57]
	Concerns over information misuse	[46]
	Concerns over lack of control on submitted information	[46]
	Concerns over unintended use of information by intruders	[46]

Table 1. *Cont.*

Nr.	Hypothesis	Relevant Study
H10	Incentives proposed by business organizations for shopping have an impact on the customer's perception of the security of online data and trust in an e-commerce application.	[47]
	Data transparency	[60]
	Encryption security	[60]
	Product return policy	[33]
	Dispute guarantee policy	[47]
	An understanding of the terms of conditions	[39]
	E-commerce platform's reputation	[39]
H11	Customers' trustworthiness of e-commerce platforms impacts the customer's perception of the security of online data and trust in an e-commerce application.	[35,41,54]
	The availability of product pictures	[41,55]
	The provision of a privacy seal on the website	[41,42]
	The provision of search feature on the website	[41,42]
	The provision of security seal on the website	[35]
	Presence of branded product logos	[41,42]
H12	Users' feelings about the reputation of e-commerce impact their perception of security of online data and trust in an e-commerce application.	[42,67]
	Users' feelings about location disclosure	[42,51]
	Users' feelings about browsing history disclosure	[42]
	Users' feelings about personal data misuse	[42]

Table 2. Parameters of the model.

PMT Constructs	Model Construct	Parameters
Perceived vulnerability	Consumer rating	CR1: Authentication of users by e-commerce websites CR2: Authentication of vendors by customers CR3: Fraud protection provisions CR4: Provision of secure communications by e-commerce websites
Response efficacy	Trustworthiness	T1: The availability of product pictures T2: The provision of a privacy seal on the website T3: The provision of search feature on the website T4: The provision of security seal on the website T5: Presence of branded product logos
Perceived severity	Credit card usage concerns	CC1: Network security issues CC2: Operating system's security issues CC3: Applications' security issues CC4: Unauthorized transaction issues CC5: Fraudulent transaction issues CC6: Disputed vendors CC7: Product quality issues

Table 2. *Cont.*

PMT Constructs	Model Construct	Parameters
Response efficacy	Motivation factors	MF1: Data transparency MF2: Encryption security MF3: Product return policy MF4: Dispute guarantee policy MF5: An understanding of the terms of conditions MF6: E-commerce platform's reputation
Response cost	Customer worries	CW1: Concerns over private information provision CW2: Concerns over information misuse CW3: Concerns over lack of control on submitted information CW4: Concerns over unintended use of information by intruders
Response cost	Customer feelings	CF1: Users' feelings about location disclosure CF2: Users' feelings about browsing history disclosure CF3: Users' feelings about personal data misuse

3. Materials and Methods

The reason for selecting Pakistan as a case setting was based on the huge potential for e-commerce growth due to a large population. We were specifically interested in developing an understanding about how people perceive privacy and security aspects in a developing country, and how these challenges can be addressed by businesses and increase their online dealings. Pakistan is the fifth biggest nation in the world, with a population of more than 225.2 million; by geographical area, it is the 33rd largest country [84]. Pakistan is the 46th largest e-commerce market in the world, with annual sales of 4 billion USD in 2020; for the next 4 years, the annual growth rate is expected to increase by another 18% [85]. According to a survey based on data obtained in 2019, the provincial shares of the net e-commerce sales were as follows: the province of Punjab had a 55% share, followed by Sindh with a 36% share, whereas other regions, Khyber Pakhtunkhwa, Balochistan, and Azad Kashmir, contributed to the remaining 9% of total e-commerce sales [86].

Our study is based on quantitative data, which are available in Appendix A, and we used PMT as a theoretical framework [18]; hence, four constructs of PMT, namely, perceived vulnerability, perceived severity, response efficacy, and response cost, were used in our questionnaire. For each of the constructs, we designed closed-ended questions on different aspects of user perception, some of which were rooted in earlier studies [87–89]. Once the questionnaire was complete, it was reviewed by two colleagues to ensure content validity. After validation, the survey was posted on Google forms. To recruit respondents, we used the nonprobability sampling method and used the snowball sampling technique by contacting our peers; the qualification criterion for the respondent was the use of e-commerce websites for online purchasing. By the end of the survey period, we received 187 responses, of which we discarded one response as the concerned respondent reported not having experience with online shopping. There were 135 male respondents and 51 female respondents, which were divided into four age groups. There were 62 respondents in the age group of 19–25 years, 51 respondents in the age group of 26–35 years, 58 respondents in the age group of 36–50 years, and 15 respondents were above 50 years old. While looking at computer knowledge, among the 186 respondents who participated in the study, 22 were beginner-level users, 63 were middle-level users, and 101 rated themselves as advanced users. The individual questions were mainly based on a five-point Likert scale (strongly disagree, disagree, neutral, disagree, and strongly disagree). Different questions were mapped to relevant constructs. Since SmartPLS only processes numeric data, the complete data file was coded into numeric data and then processed using SmartPLS [90] to identify the relevance of constructs in the model outcome. During our analysis, we applied the bootstrapping procedure, where we used the partial least squares method with 5000 iterations. The hypotheses were approved and rejected according to *p*-values.

4. Results

In this section, we discuss the data gathered during our study and the analysis we ran on it. We created a SmartPLS model for hypothesis testing, which is shown in Figure 1. In this basic model, we had latent variables of gender, age, computer proficiency, affected by the hacking, and customer's habit of checking security certificates and reading privacy certificates to understand how they affect online data security and trust in e-commerce. After the application of blindfolding, we obtained Q^2 values of 0.046 for online data security and trust in e-commerce and a value of 0.049 for the hacking victim variable; as proposed by Haier et al. [91], a value above zero indicates the model's predictive relevance.

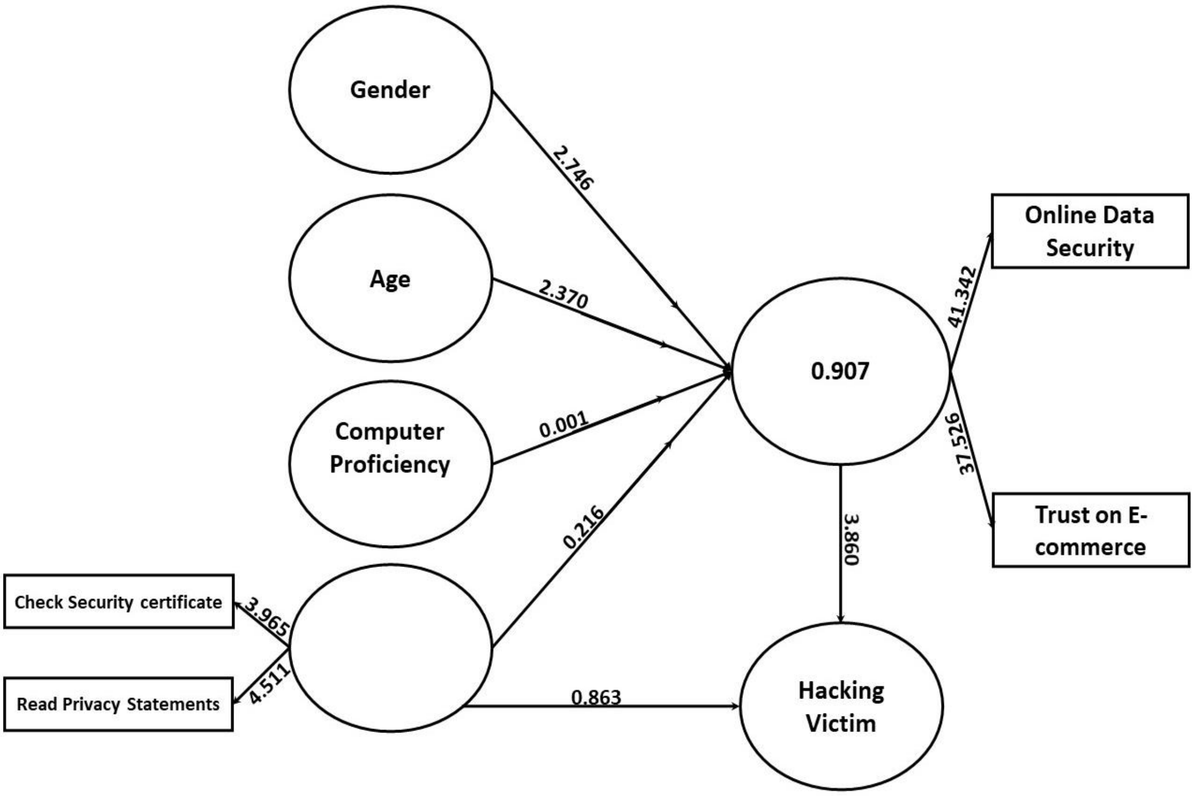

Figure 1. Basic PLS model.

To understand the detailed factors having an impact on customer perception of security and privacy, we developed a comprehensive model, as shown in Figure 2. There were six main constructs of the models, namely, consumer rating, trustworthiness, credit card usage concerns, motivation factors, customer's concerns, and customer feelings, while using the e-commerce infrastructure. The constructs were developed on the basis of different sections of our questionnaires, where each section contained a set of related questions. Each of these constructs included additional parameters highlighted in Table 2. These parameters were based on individual questions within the questionnaire. After running the analysis with the partial least squares function on SmartPLS, we found that T5, CC4, CC5, CC6, and CC7 had values less than 0.7, which means that users gave lower ratings for these factors and they were not significant factors; hence, we removed these parameters and constructed a modified model as shown in Figure 3.

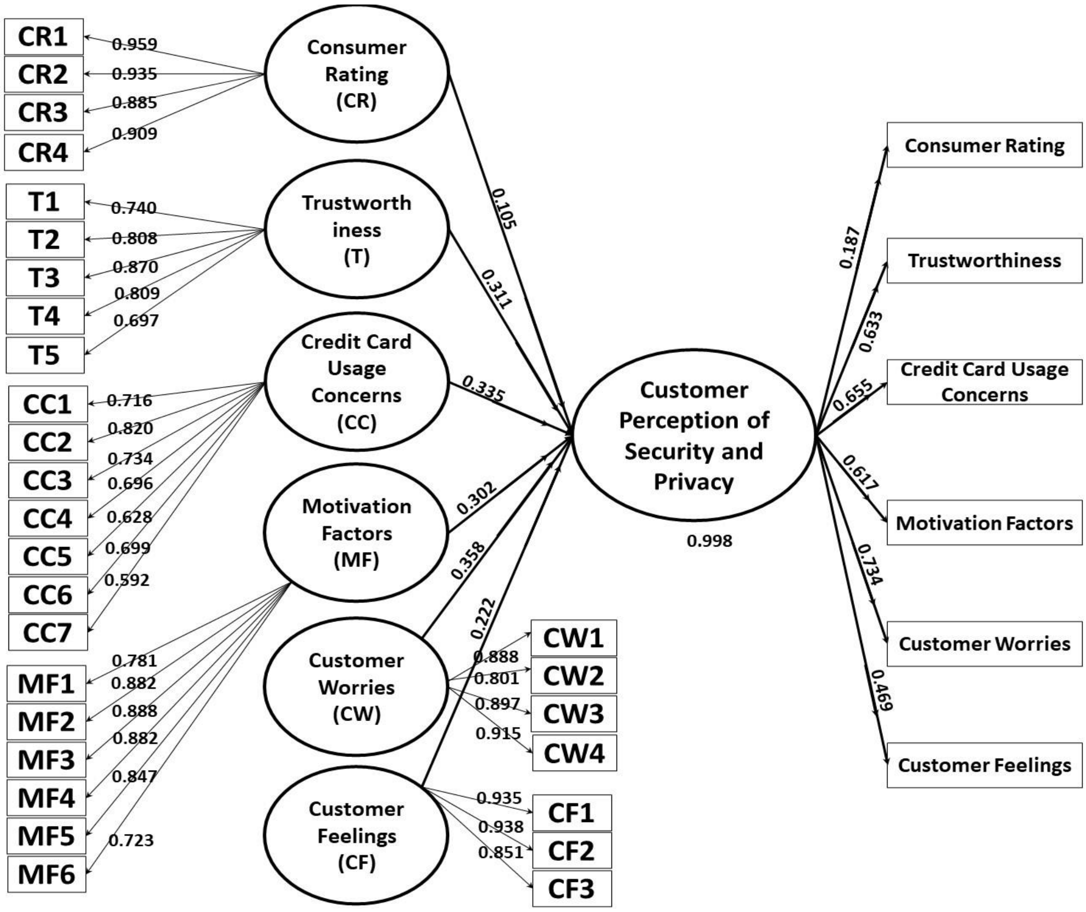

Figure 2. Detailed PLS model.

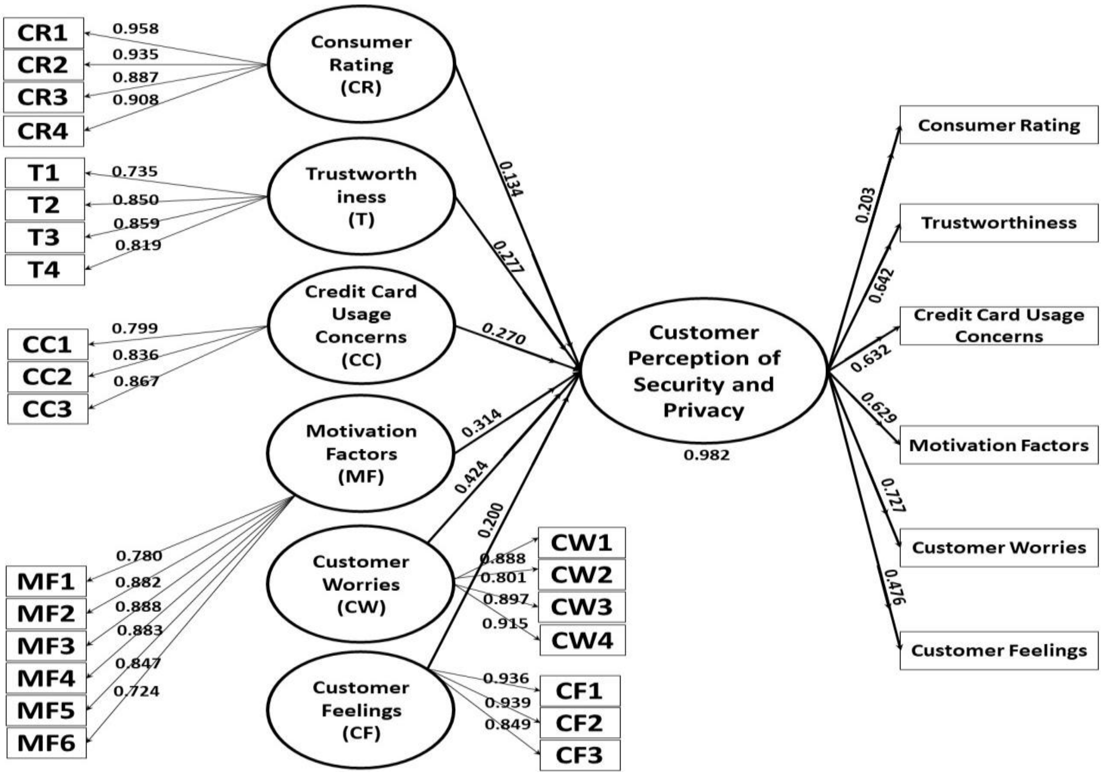

Figure 3. Revised PLS model.

Table 3 highlights the mean and standard deviation values for the constructs used in the model, which range from 0–1, showing the contribution of individual constructs to the model outcome. As shown in Table 3, the construct values were acceptable in terms of internal consistency and reliability. Cronbach's alpha value was higher than 0.7 for all constructs, showing a good internal consistency [91]; similarly, a rho value above 0.8 for all constructs confirmed the internal consistency [92]. A composite reliability above 0.7 shows good reliability, and all of our constructs achieved these values. In the case of average variance extracted (AVE), all our constructs scored greater than 0.5, which highlights the reliability of our model [93]. Q^2 values greater than 0 indicate that the model has good predictive relevance [94]. After blindfolding, we obtained a Q^2 value of 0.313 for the customer perception of security and privacy; thus, as per Hair et al., the model has predictive relevance.

Table 3. Construct consistency and reliability values.

	Mean	Std Deviation	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)	Q^2 (1 − SSE/SSO)
Consumer rating	0.128	0.085	0.942	0.994	0.958	0.851	0.728
Trustworthiness	0.265	0.041	0.832	0.832	0.889	0.668	0.44
Credit card usage concerns	0.268	0.033	0.784	0.801	0.873	0.696	0.383
Motivation factors	0.305	0.039	0.912	0.915	0.933	0.699	0.576
Customer worries	0.42	0.048	0.899	0.91	0.93	0.768	0.6
Customer feelings	0.191	0.056	0.894	0.902	0.935	0.827	0.618

The results of the path coefficient analysis are shown in Table 4. A *p*-value of less than 0.05 is normally considered as strong evidence against the null hypothesis; therefore, in our case, hypotheses 1, 2, and 5 were approved by our analysis. This implies that gender and age have an impact on the customer perception of the security and online data and their trust in e-commerce applications. Furthermore, customers having a positive perception of the security of online data and trust in e-commerce applications are less prone to hacking attacks. On the other hand, the *p*-value for H3 was 0.999, for H4 was 0.829, for H6 was 0.389, and H7 was 0.113, all of which are greater than 0.05. These higher *p*-values highlight that there was no significant evidence that computer proficiency level and reading privacy policy statements of e-commerce websites and reviewing security certificates of websites before engaging in transactions have any impact on the customers' perception of the security of online data and trust in e-commerce applications. Furthermore, there was also no evidence found that customers who read privacy policy statements of e-commerce websites and review security certificates are less prone to hacking attacks. Similarly, in the case of H7, customers' rating of the security aspects of e-commerce websites and customers' perception of the security of online data and trust in e-commerce applications were insignificant. In the cases of H8, H9, H10, H11, and H12, the *p*-values were 0, which is less than 0.05; thus, the relationship was significant, and these hypotheses were approved. Therefore, customers' credit card usage concerns, e-commerce usage concerns, shopping motivational factors by business organizations, customer trustworthiness, and user feelings about the reputation of e-commerce impact the customers' perception of the security of online data and trust in e-commerce applications.

Table 4. Hypothesis testing results.

Hypothesis	*p*-Value	Result
H1	0.006	Approved
H2	0.016	Approved
H3	0.999	Rejected
H4	0.829	Rejected
H5	0.000	Approved
H6	0.389	Rejected
H7	0.113	Rejected
H8	0.000	Approved
H9	0.000	Approved
H10	0.000	Approved
H11	0.000	Approved
H12	0.000	Approved

5. Discussion

Customer trust and positive security perception are vital for e-commerce growth in Pakistan. Our case provides emphasis on improving security aspects in e-commerce infrastructures in Pakistan. There is a need for a collective effort from all stakeholders to enhance customers' trust in e-commerce. The empirical data show that there is a need to improve customers' trust and security perception in e-commerce for Pakistani customers. Cybercrimes are considered a major factor affecting customer confidence [95]; hence, the usage of advanced digital forensic techniques and tools can help in restricting e-commerce fraud and substantially increase customer confidence [96,97]. In the case of gender, our findings support the results of Alotaibi and Alshehri [50] that gender has an impact on information security behavior, whereas our findings are contrary to the findings of McCormac et al., who found no impact of gender on information security behavior [51]. Furthermore, our results are contrary to Huang et al. [44], as we did not see any correlation between computer proficiency and customer perception. In the e-commerce context, the user and e-commerce vendor/banking infrastructure [98] are vulnerable to cybercrimes; thus, we propose to use a three-layer adoption of digital forensic tools to curb e-commerce-related crimes. Customers are vulnerable to cyberattacks; hence, periodic self-digital forensics of customers' computers and mobile devices can help to identify the presence of any malware and enhance personal security [99]. On the other hand, the adoption of digital forensic tools by e-commerce vendors and their banking partners can help them to identify, respond to, and investigate cybercrimes at the organizational level [100,101]. On the third level of government, law enforcement agencies can use digital forensic tools to investigate and respond to e-commerce frauds, and deal with criminals at the governmental level [102].

5.1. Theoretical Implications

Since cybersecurity has become very critical for the continuity of technological infrastructures, human factors are considered as issues [103]. In order to understand the security behavior of end-users, several information system theories have been employed by researchers. In the context of e-commerce, understanding user behavior is also very critical to foster a secure shopping experience. Customer motivation and security behavior are very critical for the growth of e-commerce, and our study highlights the perception of security implications of e-commerce portals in Pakistan. The findings from the study will help to perceive customers' behavior aligned with PMT constructs [23,24]; as future work, the behavior of users can be studied in line with the theory of planned behavior [104]. Such an enhanced understanding of customer behavior can help in building effective controls for e-commerce websites.

5.2. Practical Implications

On the basis of our findings, we propose a model for improving customer trust and privacy in E-commerce in Pakistan. As shown in Figure 4, we identified four important actors: customers, vendors, technology, and the government. Different actions were identified which need to be carried out by each of the actors to enhance trust and privacy of end-users. Although product quality and price competitiveness are direct contributors to customers' trust, it has been found that customers are sometimes willing to compromise their security if they find the quality and price reasonable [17]. Therefore, we recommend that vendors should provide quality products along with a competitive price as an indirect contributor to enhancing the trust of customers. Market analysis modeling tools can help in setting a price aligned with the pricing strategy of vendors [105,106]. Furthermore, if vendors have partnerships with known brands and advertise them on their website, then it also serves as a trust booster for customers [107]. Another important aspect that vendors need to pay more attention to is developing and displaying a use of information policy for all the information collected by them. If customers are aware of which information about themselves is being collected and how it will be used, it provides them with confidence about their security and privacy. Well-implemented opt-in and opt-out strategies by the e-commerce vendors show customers their sensitivity in preserving their customers' privacy. Another factor that can enhance customer trust in e-commerce websites is setting up a well-defined dispute resolution policy. Many respondents highlighted their fears that, in cases they end up with credit card fraud [49], the e-commerce vendors will not help them [108].

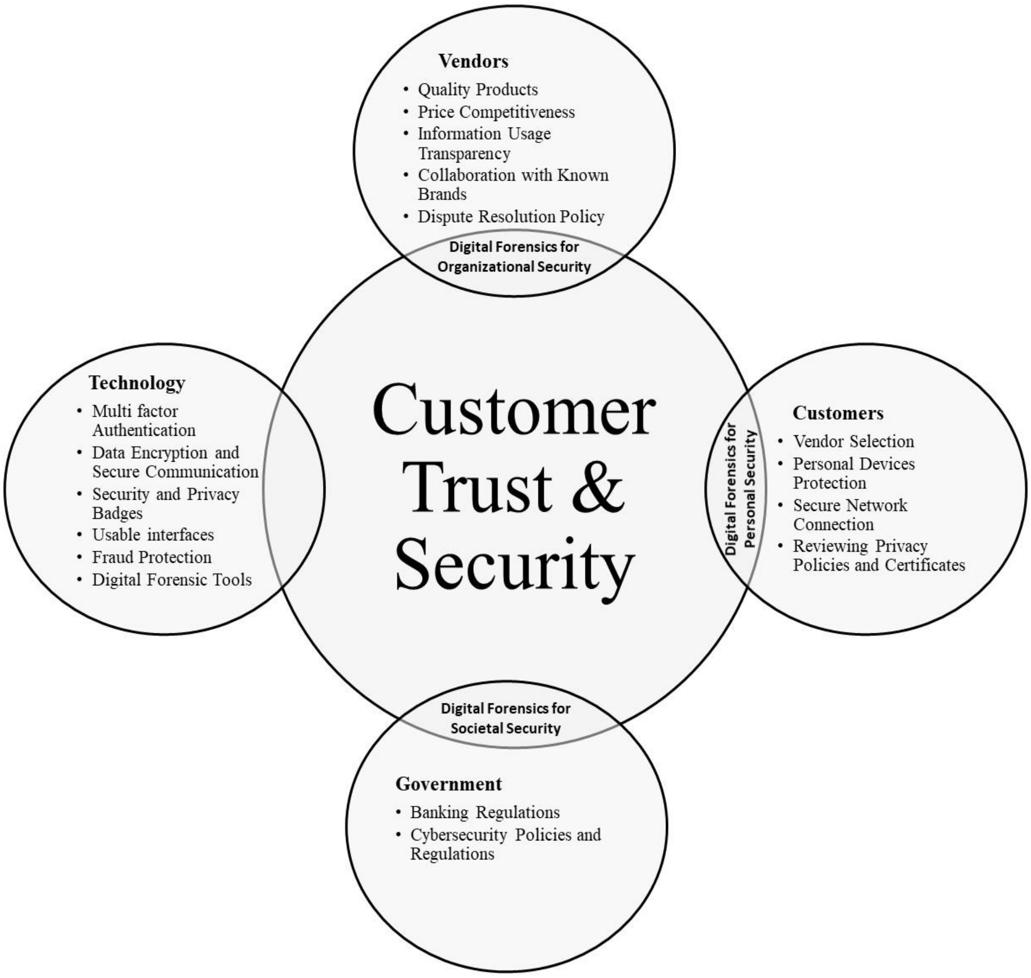
Vendors
• Quality Products
• Price Competitiveness
• Information Usage Transparency
• Collaboration with Known Brands
• Dispute Resolution Policy
Digital Forensics for Organizational Security
Technology
• Multi factor Authentication
• Data Encryption and Secure Communication
• Security and Privacy Badges
• Usable interfaces
• Fraud Protection
• Digital Forensic Tools
Customer Trust & Security
Digital Forensics for Personal Security
Customers
• Vendor Selection
• Personal Devices Protection
• Secure Network Connection
• Reviewing Privacy Policies and Certificates
Digital Forensics for Societal Security
Government
• Banking Regulations
• Cybersecurity Policies and Regulations

Figure 4. E-commerce trust and privacy enhancement model for Pakistan.

Technological infrastructure is another important factor in fostering trust and security feeling among customers. The technological infrastructure deployed by the e-commerce vendors needs to adopt data encryption algorithms and advanced technologies such as blockchain [16] to secure communication [109]. To ensure that legitimate users can use their accounts, multifactor authentication mechanisms can be helpful; hence, the e-commerce business should implement multifactor authentication for user account management. Security and privacy badges provide users with a sense of satisfaction that the e-commerce website having such badges satisfies minimum security criteria [35]. E-commerce technical infrastructure needs to be fraud-resistant so that fraudulent transactions can be proactively responded to, and the payment mechanisms are fully secure [110]. Usability is another important contributor to enhancing customer interests [46,48,79]; a well-designed e-commerce platform provides customers confidence that the website is trustworthy. Features such as enhanced product displays, detailed information, and search features provide customers with a sense of security toward the e-commerce platform. A user-centric design approach to e-commerce portals can help in improving customer usage [111–113]. Adoption of advanced forensic tools can help in real-time monitoring of the network traffic, and in extracting and preserving digital evidence against e-commerce crimes.

Customers are another important actor; to increase customer confidence, there are some activities required on part of the customers. Customers need to prescreen the e-commerce platforms before purchasing by reading reviews on different horizontal/vertical search engines and directories [114]. An enhanced presence on different intermediaries and media platforms gives users confidence about the authenticity and credibility of that e-commerce platform. Secondly, customers need to ensure that their devices, the vicinities where they connect to e-commerce websites from, and their network connection need to be secure. Empirical data showed that a large majority of customers do not read the privacy policies and security certificates of e-commerce platforms. To make their shopping experience more secure, customers should regularly read and review privacy policies and security certificates, and this practice can minimize their chances of security violations.

In the context of Pakistan, the government also needs to carry out some actions to enhance the customers' trust in e-commerce [14,15,115]. The empirical data provide evidence on customers' reservations thar, in cases of financial fraud and misuse of their data, they expect little support from banks and other relevant authorities [116,117]. Therefore, the government needs to develop cybersecurity regulations to reassure the customers that banks and other institutions will support them in cases of banking or other legal violations during their shopping experience.

At the customer level, the personal security of the technological infrastructure is critical, and digital forensic tools can help in self-diagnostics of the devices used for engaging in e-commerce activities, and computer, network, email, and malware forensic tools can be beneficial. At the e-commerce vendor level, the focus should be on organizational security to protect customer and company data. Here, computer, network, analysis, malware, email, malware, and memory tools can be critical to secure the infrastructure from unauthorized access. At the governmental level, all types of forensic tools can be used to investigate and preserve digital evidence for strict actions against e-commerce crimes.

6. Conclusions

E-commerce has affected the buying behavior of customers; however, in developing countries such as Pakistan, there is still a huge potential for its growth. Recent COVID-19-induced lockdowns and closures have provided a significant push for digital transformation in business organizations; however, customers' perception of trust and security of these websites is a vital factor for engaging in electronic business transactions. In this paper, we documented the results of an empirical study, suggesting that the age and gender of customers have an impact on the customers' perception of the security of online data and trust in e-commerce applications. Furthermore, customers who have a positive perception of the security of online data and trust in e-commerce applications are less prone to hacking attacks. They are very critical regarding privacy policies and security; thus, they pay closer attention to privacy policies and are less likely to be a victim of hacking attacks. Furthermore, we developed a model to further improve the trust and security of customers engaging in e-commerce in Pakistan.

Limitations

Our study was based on a smaller sample size which lacked gender and geographical diversity, as our sample was male-dominated, and geographical diversity was not taken into account across Pakistan. Furthermore, most respondents were advanced computer users; hence, they may have more insights into technical aspects and may be more critical of security aspects. Due to these weaknesses, the results may not be reflective of the total population; accordingly, in future studies, we intend to test the effectiveness of our model in a more comprehensive population. Since our study relied upon quantitative data, there were no detailed insights into understanding why the respondents have a certain viewpoint.

Funding: The author would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University for funding this project.

Institutional Review Board Statement: The request was approved in department of computer information systems 24th board meeting held on 13 June 2022.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The author would like to thank Tooba Nasir and Hina Gull for their support during the data collection and analysis stages of this research.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Dear Respondents,

E-commerce and social commerce are very popular in advanced countries; however, there is a lot of opportunity for the growth of E-commerce. Especially due to the COVID-19 pandemic, online shopping provides a reasonable alternative. In this study, we intend to understand how the end-users feel about the security and privacy aspects of e-commerce applications. The research data will be anonymous and will be confidential, and the results of this survey will only be used for scientific reports; the identity of users will not be revealed in any part of the report. If you are willing to help the research team by participating in the study, then proceed to record your responses for the questions.

Q1: Your Gender
Female
Male
Q2: Age?
Less than 18 Years
19–25 Years
26–35 Years
36–50 Years
Above 50 Years
Q3: How do you rate your computer proficiency (on a scale of 1–5, 1 being lowest)?
5
4
3
2
1

Q4: Do you shop online using an e-commerce website?

Yes (Go to next question)

No (Thanks, please go to end of the survey)

Q5: Which one of the following websites do you use to shop online more frequently?

○ Daraz.pk ○ Olx.com.pk ○ Homeshopping.pk ○ Symbios.pk ○ Shophive.com

○ Yayvo.com ○ 24hours.pk ○ Telemart.pk ○ iShopping.pk ○ exportleftovers.com

○ Sehgalmotors.pk ○ aliexpress.com ○ Brand's official webpage ○ Facebook/Instagram

Q6: What is your main intention for online shopping?

Low rice

Better quality product

Ease of shopping

More variety of products

Q7: Would you consider shopping online with an application/vendor that provides less security but has decreased product prices?

Yes (Go to next question)

No (Thanks, please go to end of the survey)

Q8: In general, how secure do you feel your data are online (on a scale of 1–5, 1 being lowest)?

5

4

3

2

1

Q9: On a scale of 1–5, how much do you trust eCommerce platforms?

5

4

3

2

1

Q10: Have you ever been a victim of a hacking attack?

Yes

No

Q11: In case you answered yes to the previous question, then did the experience of being hacked change the way you shop online?

Yes

No

Q12: Do you check policies, certificate of shopping apps and their companies before entering credit card details/personal information?

Yes

No

Q13: Do you read the privacy policy statement before accepting it?

Yes

No

Q14: As a consumer, how do you rank on a scale of 1–5 (1 being lowest) the following security features of an e-commerce website:

Provision of secure communication	5	4	3	2	1
Authentication of users by vendor platforms	5	4	3	2	1
Authentication of vendor platforms by users	5	4	3	2	1
Fraud protection provision by vendor platforms	5	4	3	2	1

Q15: Which of the following visible factors would increase the trustworthiness of a website and, hence, influence you to purchase from that website (rank on a scale of 1–5, 1 being lowest)?

Availability of product pictures	5	4	3	2	1
Provision of security seals (using https in address and security badges)	5	4	3	2	1
Provision of privacy seals (using trust and privacy badges)	5	4	3	2	1
Provision of search facility	5	4	3	2	1
Presence of logos of well-known brand	5	4	3	2	1

Q16: When you have the intention to buy something through an e-commerce website using your credit card, which of the following is a relevant concern (rank on a scale of 1–5, 1 being lowest)?

Someone might perform unauthorized transactions if your device is stolen or lost	5	4	3	2	1
The network you use (4G, 3G, and Wi-Fi) have security deficiencies	5	4	3	2	1
Your system has operating system security deficiencies	5	4	3	2	1
E-commerce website has security deficiencies	5	4	3	2	1
The quality of the delivered product might not be as it was anticipated	5	4	3	2	1
There is a possibility of fraudulent transactions in your credit card	5	4	3	2	1
E-commerce vendor’s reputation is disputed	5	4	3	2	1

Q17: When you are leaning toward buying something online, which of the following factors is more relevant in increasing your motivation to do online buying (rank on a scale of 1–5, 1 being lowest)?

Data transparency	5	4	3	2	1
Encryption security	5	4	3	2	1
Product return policy	5	4	3	2	1
Dispute guarantee policy	5	4	3	2	1
An understanding of the terms of conditions	5	4	3	2	1
E-commerce platform’s reputation	5	4	3	2	1

Q18: I am concerned that the information I submit on the internet could be misused
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q19: I am concerned that a person can find private information about me on the internet.
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q20: I am concerned about submitting information on the internet, because of what others might do with it.
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q21: I am concerned about submitting information on the internet, because it could be used in a way I did not foresee.

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q22: I am concerned if my device reveals information about my current location

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q23: I am concerned that my device reveals information about my preferences or browsing history.

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

Q24: I am concerned that my personal data might be used by the retailer for a secondary purpose such as marketing products or services.

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

You have reached to the end of questionnaire. We are very thankful to you for spending time in filling out responses. You can reach us by email to receive findings once we finish the study.

References

1. Danneels, E. Disruptive Technology Reconsidered: A Critique and Research Agenda. *J. Prod. Innov. Manag.* **2004**, *21*, 246–258. [CrossRef]
2. Jelassi, T.; Martínez-López, F.J. Strategic Trends for e-Business. In *Strategies For E-Business*; Springer: Cham, Switzerland, 2020; pp. 501–533.
3. Ortiz, J. The global environment through the SLEPT framework. *Int. J. Bus. Glob.* **2010**, *5*, 475–492. [CrossRef]
4. Chaffey, D.; Edmundson-Bird, D.; Hemphill, T. *Digital Business and E-Commerce Management*; Pearson: London, UK, 2019.
5. Bhatti, A.; Akram, H.; Basit, H.M.; Khan, A.U.; Raza, S.M.; Naqvi, M.B. E-commerce trends during COVID-19 Pandemic. *Int. J. Future Gener. Commun. Netw.* **2020**, *13*, 1449–1452.
6. Saeed, S.; Rodríguez Bolívar, M.P.; Ramayah, T. *Pandemic, Lockdown, and Digital Transformation: Challenges and Opportunities for Public Administration, NGOs, and Businesses*; Springer: Berlin/Heidelberg, Germany, 2021; ISBN 978-3-03086-273-2. [CrossRef]
7. Akram, U.; Fülöp, M.T.; Tiron-Tudor, A.; Topor, D.I.; Căpușneanu, S. Impact of Digitalization on Customers' Well-Being in the Pandemic Period: Challenges and Opportunities for the Retail Industry. *Int. J. Environ. Res. Public Health* **2021**, *18*, 7533. [CrossRef] [PubMed]
8. Gu, S.; Ślusarczyk, B.; Hajizada, S.; Kovalyova, I.; Sakhbieva, A. Impact of the COVID-19 Pandemic on Online Consumer Purchasing Behavior. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 2263–2281. [CrossRef]
9. Guthrie, C.; Fosso-Wamba, S.; Arnaud, J.B. Online consumer resilience during a pandemic: An exploratory study of e-commerce behavior before, during and after a COVID-19 lockdown. *J. Retail. Consum. Serv.* **2021**, *61*, 102570. [CrossRef]
10. Shu, S.; Liu, Y. Looking Back to Move Forward: A Bibliometric Analysis of Consumer Privacy Research. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 727–747. [CrossRef]
11. Connolly, R.; Bannister, B. E-Commerce Trust Beliefs: The Influence of National Culture. In Proceedings of the European and Mediterranean Conference on Information Systems (EMCIS 2007), Valencia, Spain, 24–26 June 2007.
12. Mohammed, Z.A.; Tejay, G.P. Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. *Comput. Secur.* **2017**, *67*, 254–265. [CrossRef]

13. Clemons, E.K.; Wilson, J.; Matt, C.; Hess, T.; Ren, F.; Jin, F.; Koh, N.S. Global Differences in Online Shopping Behavior: Understanding Factors Leading to Trust. *J. Manag. Inf. Syst.* **2016**, *33*, 1117–1148. [CrossRef]
14. Teo, T.S.; Liu, J. Consumer trust in e-commerce in the United States, Singapore and China. *Omega* **2007**, *35*, 22–38. [CrossRef]
15. Worzala, E.M.; McCarthy, A.M.; Dixon, T.; Marston, A. E-commerce and retail property in the UK and USA. *J. Prop. Investig. Finance* **2002**, *20*, 142–158. [CrossRef]
16. Koroma, J.; Rongting, Z.; Muhideen, S.; Akintunde, T.Y.; Amosun, T.S.; Dauda, S.J.; Sawaneh, I.A. Assessing citizens' behavior towards blockchain cryptocurrency adoption in the Mano River Union States: Mediation, moderation role of trust and ethical issues. *Technol. Soc.* **2022**, *68*, 101885. [CrossRef]
17. Bylok, F. Examining the Impact of Trust on the e-Commerce Purchase Intentions of Young Consumers in Poland. *J. Internet Commer.* **2021**, *21*, 364–391. [CrossRef]
18. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* **1975**, *91*, 93–114. [CrossRef]
19. Kim, J.; Yang, K.; Min, J.; White, B. Hope, fear, and consumer behavioral change amid COVID-19: Application of protection motivation theory. *Int. J. Consum. Stud.* **2022**, *46*, 558–574. [CrossRef]
20. Ong, A.K.S.; Prasetyo, Y.T.; Salazar, J.M.L.D.; Erfe, J.J.C.; Abella, A.A.; Young, M.N.; Chuenyindee, T.; Nadlifatin, R.; Redi, A.A.N.P. Investigating the acceptance of the reopening bataan nuclear power plant: Integrating protection motivation theory and extended theory of planned behavior. *Nucl. Eng. Technol.* **2022**, *54*, 1115–1125. [CrossRef]
21. Preissner, C.E.; Kaushal, N.; Charles, K.; Knäuper, B. A Protection Motivation Theory Approach to Understanding How Fear of Falling Affects Physical Activity Determinants in Older Adults. *J. Gerontol. Ser. B Psychol. Sci. Soc. Sci.* **2022**, *2*, gbac105. [CrossRef]
22. Gumasing, M.J.J.; Prasetyo, Y.T.; Ong, A.K.S.; Nadlifatin, R. Determination of factors affecting the response efficacy of Filipinos under Typhoon Conson 2021 (Jolina): An extended protection motivation theory approach. *Int. J. Disaster Risk Reduct.* **2022**, *70*, 102759. [CrossRef]
23. Dang-Pham, D.; Pittayachawan, S. Comparing intention to avoid malware across contexts in a BYOD-enabled Aus-tralian university: A protection motivation theory approach. *Comput. Secur.* **2015**, *48*, 281–297. [CrossRef]
24. Verkijika, F.S. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Comput. Secur.* **2018**, *77*, 860–870. [CrossRef]
25. Chiu, C.M.; Cheng, H.L.; Hsu, J.; Huang, C.H. Examining Employees' Intention to Comply with Information Security Policies: The Roles of Loafing and Commitment. In Proceedings of the Pacific Asia Virtual Conference on Information System, Virtual, July 5–9 2022. paper 1158.
26. Kim, S.-K. Enhanced Stochastic Methodology for Combined Architecture of E-Commerce and Security Networks. *Math. Probl. Eng.* **2009**, *2009*, 691680. [CrossRef]
27. Qiu, L.; Li, J. Covering the Monitoring Network: A Unified Framework to Protect E-Commerce Security. *Complexity* **2017**, *2017*, 6254842. [CrossRef]
28. Hussien, F.T.A.; Rahma, A.M.S.; Wahab, H.B.A. A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites. *Secur. Commun. Networks* **2021**, *2021*, 9961172. [CrossRef]
29. Hassan, A.; Shukur, Z.; Hasan, M.K.; Hassan, A. An Efficient Secure Electronic Payment System for E-Commerce. *Computers* **2020**, *9*, 66. [CrossRef]
30. Chen, T.-C.; Liang, Y.-S.; Ko, P.-S.; Huang, J.-C. Optimization Model of Cross-Border E-commerce Payment Security by Blockchain Finance. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9192219. [CrossRef]
31. Liu, J.; Gu, X.; Shang, C. Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data. *Complexity* **2020**, *2020*, 6685888. [CrossRef]
32. Nanduri, J.; Jia, Y.; Oka, A.; Beaver, J.; Liu, Y.-W. Microsoft Uses Machine Learning and Optimization to Reduce E-Commerce Fraud. *INFORMS J. Appl. Anal.* **2020**, *50*, 64–79. [CrossRef]
33. Shah, S.A.M.; Jadoon, M.S.-U.; Tahir, M.; Anwar, J. Examining the Trust-Based Consumer Decision-Making Model for Online Purchases in Pakistan. *Int. J. Online Mark.* **2021**, *11*, 41–62. [CrossRef]
34. Liu, D.; Li, M. Exploring new factors affecting purchase intention of mobile commerce: Trust and social benefit as mediators. *Int. J. Mob. Commun.* **2019**, *17*, 108–125. [CrossRef]
35. Jiménez, D.L.; Dittmar, E.; Portillo, J.V. The Use of Trust Seals in European and Latin American Commercial Transactions. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 150. [CrossRef]
36. Dhende, K.; Meshram, S. Review of e-Commerce Security Challenges. *Turk. J. Comput. Mathe-Matics Educ. (TURCOMAT)* **2021**, *12*, 3593–3598.
37. Tan, Y.C.L. Recent Technological Trends and Security Challenges in Trust-Building in E-Commerce. *Int. J. Bus. Manag.* **2021**, *14*, 226.
38. Zhang, H.D.; Chen, S.C.; Ruangkanjanases, A. Benefits First: Consumer Trust Repair in Mobile Commerce. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 1079–1096. [CrossRef]
39. Turner, C.W.; Zavod, M.; Yurcik, W. Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites. In Proceedings of the Fourth International Conference on Electronic Commerce Research, Dallas, TX, USA, 8–11 November 2001; pp. 628–636.
40. Liebermann, Y.; Stashevsky, S. Perceived risks as barriers to Internet and e-commerce usage. *Qual. Mark. Res. Int. J.* **2002**, *5*, 291–300. [CrossRef]

41. Belanger, F.; Hiller, J.S.; Smith, W.J. Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *J. Strat. Inf. Syst.* **2002**, *11*, 245–270. [CrossRef]
42. Yenisey, M.M.; Ozok, A.; Salvendy, G. Perceived security determinants in e-commerce among Turkish university students. *Behav. Inf. Technol.* **2005**, *24*, 259–274. [CrossRef]
43. McDonald, A.M.; Cranor, L.F. The cost of reading privacy policies. *I/S J. Law Policy Inf. Soc.* **2008**, *4*, 543.
44. Huang, D.-L.; Rau, P.-L.P.; Salvendy, G. Perception of information security. *Behav. Inf. Technol.* **2010**, *29*, 221–232. [CrossRef]
45. Beldad, A.; de Jong, M.; Steehouder, M. Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. *Gov. Inf. Q.* **2010**, *27*, 238–244. [CrossRef]
46. Bonera, M. The propensity of e-commerce usage: The influencing variables. *Manag. Res. Rev.* **2011**, *34*, 821–837. [CrossRef]
47. Chowdhury, E.K.; Chowdhury, R. Online shopping in Bangladesh: A study on the motivational factors for ecommerce that influence shopper's affirmative tendency towards online shopping. *South Asian J. Mark. Manag. Res.* **2017**, *7*, 20–35. [CrossRef]
48. Kasuma, J.; Kanyan, A.; Khairol, M.; Sa'ait, N.; Panit, G. Factors influencing customers intention for online shopping. *Int. J. Mod. Trends Bus. Res.* **2020**, *3*, 31–41.
49. Zahrani, A.A. Consumers' perceptions of intention to use a credit card: Perceived risk and security. *Entrep. Sustain. Issues* **2021**, *9*, 37–49. [CrossRef] [PubMed]
50. Alotaibi, F.; Alshehri, A. Gender Differences in Information Security Management. *J. Comput. Commun.* **2020**, *8*, 53–60. [CrossRef]
51. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. *Comput. Hum. Behav.* **2017**, *69*, 151–156. [CrossRef]
52. Tang, Z.; Miller, A.S.; Zhou, Z.; Warkentin, M. Does government social media promote users information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Gov. Inf. Q.* **2021**, *38*, 101572. [CrossRef]
53. Yazdanifard, R.; Edres, N.A.H.; Seyedi, A.P. Security and privacy issues as a potential risk for further ecommerce development. In Proceedings of the International Conference on Information Communication and Management-IPCSIT, Singapore, 14 October 2011; Volume 16. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=01c55d28035e91cb5882bda08cb599cc63f44578 (accessed on 30 November 2022).
54. Jensen, C.D. The importance of trust in computer security. In *IFIP International Conference on Trust Management*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–12.
55. Saeed, S. Digital Business adoption and customer segmentation: An exploratory study of expatriate community in Saudi Arabia. *ICIC Express Lett.* **2019**, *13*, 133–139.
56. Gupta, G.; Nage, A. Analyzing the Best Security Mechanism that should be Implemented by E-Commerce Business. *Int. Res. J. Eng. Technol. (IRJET)* **2021**, *8*, 2393–2398.
57. Mason, R.O. Four Ethical Issues of the Information Age. *MIS Q.* **1986**, *10*, 5–12. [CrossRef]
58. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Saqib, M.; Al Qahtani, S.H.; Alamer, A. An Empirical Study of Mobile Commerce and Customers Security Perception in Saudi Arabia. *Electronics* **2022**, *11*, 293. [CrossRef]
59. Khan, M.M.; RoJa, N.T.; Almalki, F.A.; Aljohani, M. Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract. *Secur. Commun. Netw.* **2022**, *2022*, 2213336. [CrossRef]
60. Gouthier, M.H.; Nennstiel, C.; Kern, N.; Wendel, L. The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce. *J. Bus. Res.* **2022**, *148*, 174–189. [CrossRef]
61. Mashatan, A.; Sangari, M.S.; Dehghani, M. How Perceptions of Information Privacy and Security Impact Consumer Trust in Crypto-Payment: An Empirical Study. *IEEE Access* **2022**, *10*, 69441–69454. [CrossRef]
62. Vuță, D.R.; Nichifor, E.; Țierean, O.M.; Zamfirache, A.; Chițu, I.B.; Foris, T.; Brătucu, G. Extending the Frontiers of Electronic Commerce Knowledge through Cybersecurity. *Electronics* **2022**, *11*, 2223. [CrossRef]
63. Masyhuri, M. Key Drivers of Customer Satisfaction on the E-Commerce Business. *EAJMR East Asian J. Multidiscip. Res.* **2022**, *1*, 657–670. [CrossRef]
64. Alkis, A.; Kose, T. Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. *Comput. Hum. Behav.* **2022**, *137*, 107412. [CrossRef]
65. Anshori, M.Y.; Karya, D.F.; Gita, M.N. A Study on the Reuse Intention of E-Commerce Platform Applications: Security, Privacy, Perceived Value, and Trust. *J. Manaj. Teor. Dan Terap. J. Theory Appl. Manag.* **2022**, *15*, 13–24. [CrossRef]
66. Cebeci, S.E.; Nari, K.; Ozdemir, E. Secure E-Commerce Scheme. *IEEE Access* **2022**, *10*, 10359–10370. [CrossRef]
67. Novita, D.; Budiarti, A.P. Perceived security, trust, privacy, and continuance intention of e-commerce customer. *Oper. Manag. Inf. Syst. Stud.* **2022**, *2*, 1–13.
68. Marett, K.; Mcnab, A.L.; Harris, R.; Marett, K.; Harris, R. Social networking websites and posting personal infor-mation: An evaluation of protection motivation theory. *AIS Trans. Hum. Comput. Interact.* **2011**, *3*, 170–188. [CrossRef]
69. Meso, P.; Ding, Y.; Xu, S. Applying Protection Motivation Theory to Information Security Training for College Students. *J. Inf. Priv. Secur.* **2013**, *9*, 47–67. [CrossRef]
70. Hanus, B.; Wu, Y. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Inf. Syst. Manag.* **2015**, *33*, 2–16. [CrossRef]
71. Erhart, M.A. Protection Motivation Theory Interactions in Small Business Employees' Security Policy Compliance. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2022.

72. Ganesh, A.; Ndulue, C.; Orji, R. Smartphone Security and Privacy—A Gamified Persuasive Approach with Protection Motivation Theory. In *International Conference on Persuasive Technology*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 89–100. [CrossRef]
73. Mou, J.; Cohen, J.; Bhattacherjee, A.; Kim, J. A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising. *J. Assoc. Inf. Syst.* **2022**, *23*, 196–236. [CrossRef]
74. Khan, W.A.; Yousaf, S.; Mian, N.A.; Nawaz, Z. E-commerce in Pakistan: Growth Potentials and E-Payment Solutions. In Proceedings of the 2013 11th International Conference on Frontiers of Information Technology, Washington, DC, USA, 16–18 December 2013; pp. 247–252.
75. Arshad, M.; Zaidi, S.S.Z. Role of electronic commerce (E-commerce) in Pakistan: Consumer behavior, growth prospects, and challenges. *Int. J. Manag. (IJM)* **2020**, *11*, 264–278.
76. Ghouri, M.W.A.; Hussain, M.A.; Kanwal, T.; Afzal, B.; Rasheed, M. Influence of E-Commerce on Business Growth in Pakistan: An Approach to Analyze Privacy, Threats and Consumer Trust in Business. *Int. J. Comput. Sci. Issues (IJCSI)* **2018**, *15*, 27–35.
77. Anjum, S.; Chai, J. Drivers of Cash-on-Delivery Method of Payment in E-Commerce Shopping: Evidence From Pakistan. *SAGE Open* **2020**, *10*, 2158244020917392. [CrossRef]
78. Tanveer, M. Analytical approach on small and medium Pakistani business based on E-Commerce Ethics with effect on customer repurchase objectives and loyalty. *J. Leg. Ethical Regul. Issues* **2021**, *24*, 1–20.
79. Saeed, S.; Wahab, F.; Cheema, S.A.; Ashraf, S. Role of usability in e-government and e-commerce portals: An empirical study of Pakistan. *Life Sci. J.* **2013**, *10*, 8–13.
80. Agren, E.S.; Barbutiu, S.M. Barriers in the adoption of e-commerce in Pakistan with the focus on Gender. *Int. J. Sci. Technol. Res.* **2018**, *7*, 23–31.
81. Ahmed, R. Ecommerce in Pakistan: Challenges Opportunities. WHICEB 2019 Proceedings. 75. 2019. Available online: https://aisel.aisnet.org/whiceb2019/75 (accessed on 30 November 2022).
82. Amjad, T.; Rani, S.H.A.; SaAtar, S. A New Dimension of Entrepreneurial Marketing and Key Challenges: A Case Study from Pakistan. *SEISENSE J. Manag.* **2020**, *3*, 1–14. [CrossRef]
83. Imtiaz, S.; Ali, S.H.; Kim, D.J. E-Commerce Growth in Pakistan: Privacy, Security, and Trust as Potential Issues. *Culin. Sci. Hosp. Res.* **2020**, *26*, 10–18.
84. The eCommerce Market in Pakistan. Available online: https://ecommercedb.com/en/markets/pk/all (accessed on 30 November 2022).
85. What Do we Know About Pakistan's Ecommerce Industry? Available online: https://www.dawn.com/news/1549691 (accessed on 30 November 2022).
86. Available online: https://en.wikipedia.org/wiki/Pakistan (accessed on 30 November 2022).
87. Furnell, S.; Karweni, T. Security implications of electronic commerce: A survey of consumers and businesses. *Internet Res.* **1999**, *9*, 372–382. [CrossRef]
88. Balzer, F.; Bollig, B. Perception of Data Security in E-Commerce. Ph.D. Thesis, Hochschule Furtwangen University, Furtwangen im Schwarzwald, Germany, 2020.
89. Rigopoulou, A. What is the Link Between Social Network Activity and Online Conspicuous Consumption? Master's Thesis, Erasmus University, Rotterdam, The Netherlands, 2014. Available online: https://thesis.eur.nl/pub/17587/Rigopoulou-A.-369962ar-.doc (accessed on 26 December 2022).
90. Ringle, C.; Da Silva, D.; Bido, D. Structural Equation Modeling with the SmartPLS. *Braz. J. Mark.* **2014**, *13*, 1–18.
91. Hair, J.F., Jr.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]
92. Srinivasan, R.; Lilien, G.L.; Rangaswamy, A. Technological Opportunism and Radical Technology Adoption: An Application to E-Business. *J. Mark.* **2002**, *66*, 47–60. [CrossRef]
93. Khoshkam, M. Residents' Attitude Towards Impacts from Tourism Development in Anzali Wetland, Iran. Ph.D. Thesis, University Sains Malaysia, Gelugor, Malaysia, 2013.
94. Chin, W.W. The Partial Least Squares approach for structural equation modelling. In *Modern Methods for Business Research*; Marcoulides, G.A., Ed.; Lawrence Erlbaum: Mahwah, NJ, USA, 1998; pp. 295–336.
95. Apau, R.; Koranteng, F.N.; Gyamfi, S.A. Cyber-Crime and its Effects on E-Commerce Technologies. *J. Inf.* **2019**, *5*, 39–59. [CrossRef]
96. Ward, E.D. The Influence of Mobile Technology Advancements on Digital Forensics Investigations Practices and Procedures: A Generic Qualitative Inquiry. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2021.
97. Fianyi, I. Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. *arXiv* **2016**, arXiv:1610.08369.
98. Goel, S. Cyber-Crime: A growing threat to Indian banking sector. In Proceedings of the 3rd International Conference on Recent Innovations in Science, Technology, Management and Environment, New Delphi, India, 18 December 2016; pp. 13–22.
99. Vujačić, I.; Ognjanović, I.; Šendelj, R. SM@ RT Home Personal Security and Digital Forensic Issues. In Proceedings of the Eight International Conference on Business Information Security, Belgrade, Serbia, 15 October 2016.
100. Englbrecht, L.; Meier, S.; Pernul, G. Towards a capability maturity model for digital forensic readiness. *Wirel. Netw.* **2019**, *26*, 4895–4907. [CrossRef]
101. Ariffin, K.A.Z.; Ahmad, F.H. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4. *Comput. Secur.* **2021**, *105*, 102237. [CrossRef]
102. Parker, C.M. Exploring the Use of Information Security Practices in Response to Cyberattacks to Protect US Federal Systems and Networks. Ph.D. Thesis, Northcentral University, Scottsdale, AZ, USA, 2021.

103. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
104. Sommestad, T.; Karlzén, H.; Hallberg, J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf. Comput. Secur.* **2015**, *23*, 200–217. [CrossRef]
105. Kumari, J.J.A.; Gotmare, P.R. Price Transparency Issues and Treating Customer Fairly by E-Commerce Firms in India. *J. Contemp. Issues Bus. Gov.* **2021**, *27*, 1403–1413.
106. Nguyen, T. Market Analysis for Product Selection. A case study of the eCommerce business, Zertta. Bachelor's Thesis, Laurea University of Applied Sciences, Vantaa, Finland, 2021.
107. Basit, A.; Yee, A.L.W.; Sethumadhavan, S.; Rajamanoharan, I.D. The influence of Social Media Marketing on Consumer Buying Decision through Brand Image in the Fashion Apparel Brands. *New Arch Int. J. Contemp. Archit.* **2021**, *8*, 564–576.
108. Turel, O.; Yuan, Y. Online Dispute Resolution Services: Justice, Concepts, and Challenges. In *Handbook of Group Decision and Negotiation*; Springer: Berlin/Heidelberg, Germany, 2021. [CrossRef]
109. Chauhan, E. AES encryption and MD5 hash function along with steganography to make secure money transaction. *Res. Cell Int. J. Eng. Sci.* **2016**, *18*, 87–99.
110. Fernandes, L. Fraud in electronic payment transactions: Threats and countermeasures. *Asia Pac. J. Mark. Manag. Review* **2013**, *2*, 23–32.
111. Saeed, S.; Bajwa, I.S.; Mahmood, Z. *Human Factors in Software Development and Design*; IGI Global: Hershey, PA, USA, 2014.
112. Saeed, S.; Bamarouf, Y.A.; Ramayah, T.; Iqbal, S.Z. *Design Solutions for User-Centric Information Systems*; IGI Global: Hershey, PA, USA, 2016.
113. Ashraf, N.; Faisal, C.N.; Jabbar, S.; Habib, M.A.; Kiran, I.; Ahmad, M. The Effect of Website Design Artifacts and Emotions on Behavioral Purchase Intention in M-Commerce. In Proceedings of the 2019 8th International Conference on Infor-mation and Communication Technologies (ICICT), Karachi, Pakistan, 16 November 2019; pp. 100–105. [CrossRef]
114. Sohail, S.S.; Siddiqui, J.; Ali, R. Product Recommendation Techniques for Ecommerce-past, present and future. *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)* **2012**, *1*, 219.
115. Ghoneim, A.; Ghoneim, S.; Kamel, S. The Role of the Government in eCommerce in Egypt. In Proceedings of the International Research Foundation for Development (IRFD); Conference of the UN World Summit on Information Society, Geneva, Switzerland, 10–12 December 2003.
116. Mwasomola, U.L.; Ojwang, E.; Pastory, D. *Examining the Consumer Protection and Comprehensiveness in Ecommerce in Tanzania*; CBE: Dar, Tanzania, 2020.
117. Ololade, B.M.; Salawu, M.K.; Adekanmi, A.D. E-Fraud in Nigerian Banks: Why and How? *J. Financ. Risk Manag.* **2020**, *9*, 211–228. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.