



Article

Comprehensive Privacy Awareness Framework (CPAF): Assessing Privacy Awareness of Saudi E-Commerce Users

Norah D. Alotaibi ^{1,2,*} , Maysoon Abulkhair ¹ and Manal Bayousef ¹

¹ Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia

² Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia

* Correspondence: nalotaibi0385@stu.kau.edu.sa

Abstract

With the rapid expansion of the Internet, it is crucial to be aware of the different aspects of privacy, especially in light of rising global cybersecurity threats and data breaches. While previous research has identified various factors when studying privacy awareness, these studies often remain fragmented or examine key factors in isolation from one another, limiting their ability to provide a holistic view. To address this gap, this study proposes the Comprehensive Privacy Awareness Framework (CPAF), which is a theoretically grounded model that conceptualizes privacy awareness across four dimensions: individual, technological, organizational, and social. The framework is empirically validated through a case study of Saudi e-commerce users, a context chosen due to the sector's rapid digital transformation under Vision 2030 and limited comprehensive privacy research. A CPAF-based survey was administered to 400 active e-commerce users. The quantitative results demonstrate that privacy awareness is a multidimensional construct, where each dimension is significantly associated with the others. Privacy awareness cannot be captured through a single and uniform measure. The findings further reveal notable gaps in users' knowledge, behaviors, and perceptions of privacy risks, indicating insufficient preparedness when navigating e-commerce environments. These insights highlight the urgent need for targeted awareness initiatives and policy interventions to strengthen user protection and foster responsible digital participation.

Keywords: cybersecurity; privacy and security; privacy awareness; e-commerce security; human factors; user behavior; data protection; Saudi Arabia



Academic Editor: Ercan Oztemel

Received: 4 December 2025

Revised: 9 January 2026

Accepted: 19 January 2026

Published: 2 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Privacy has become one of the most critical issues in today's digital world. Privacy is the user's right to keep their personal information confidential and maintain control over it [1]. However, this right is constantly under threat. Every time users browse the internet, use social media, or even shop online, their personal data can be collected, stored, sold, and used by various companies. This data may include general information, like names, or sensitive information, such as credit card details. Companies typically use this data for various purposes, such as targeted advertising, marketing, and even improving the quality of the services provided [2]. However, this information can be vulnerable to misuse, abuse, and even breaches. For instance, hackers recently stole nearly 13,000 credit card numbers and passwords from well-known websites, such as Walmart and Amazon [3].

Users should be aware of such risks so that they can make informed and intelligent decisions about their online activities. This need for awareness has caught the attention of researchers and led to the concept of “privacy awareness”. Although there is no unified definition of this concept, it generally refers to an individual’s understanding of privacy issues, including their awareness of related regulations and policies [4–7]. In the literature, this is considered to be a complex construct that is studied and measured from different angles and using various factors.

While privacy awareness has been widely investigated and measured in fields, such as the Internet of Things (IoT) and social media [8–15], research in other areas, such as e-commerce platforms, especially in Saudi Arabia, remains limited [16,17]. This gap is concerning, given the rapid expansion of e-commerce worldwide, especially after the COVID-19 pandemic [17,18]. In the Middle East, specifically in Saudi Arabia, the e-commerce sector has also experienced significant growth. According to the Ministry of Commerce [19], in 2019, Saudi Arabia ranked 9th for e-commerce growth improvement among Asian countries and 49th in the United Nations (UN) E-commerce Index. Additionally, in 2021, the number of online stores increased to 36,447 stores, as shown in Figure 1. At the end of 2024, the number of electronic commercial registrations in Saudi Arabia reached approximately 40,913, according to the annual report of the Ministry of Commerce (<https://mc.gov.sa/ar/About/Statistics>, accessed on 4 December 2025.).

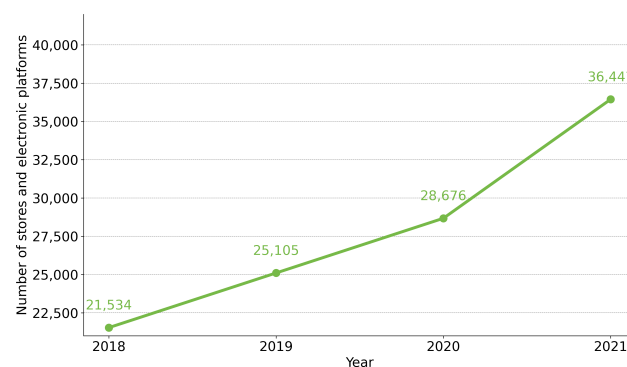


Figure 1. The Development of the Number of E-commerce Stores and Platforms in Saudi Arabia During the Period (2018–2021) [20,21].

With the growth of these stores, the number of users has also reached a new level. Recent statistics reveal that the percentage of online shoppers in Saudi Arabia exceeds 60% [22,23]. As can be seen in Figure 2, the number of e-commerce users is expected to reach 34.5 million by 2025. Therefore, there is a critical need to study and investigate the complex state of privacy awareness among e-commerce platform users.

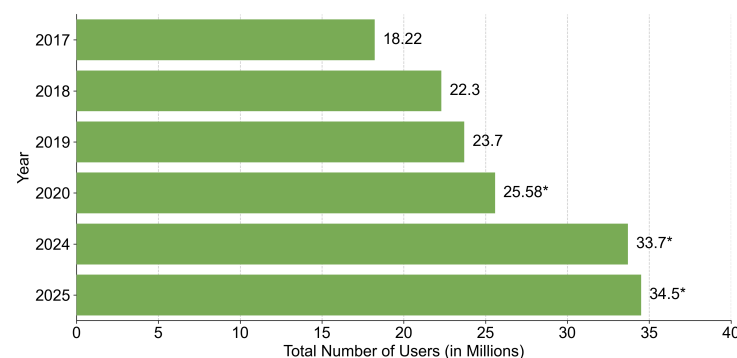


Figure 2. Growth in the Number of E-commerce Users in Saudi Arabia from 2017 to 2025* (* Expected) [24,25].

This study will begin by introducing the Comprehensive Privacy Awareness Framework (CPAF), as a new and flexible framework designed to be adaptable to various regulatory and cultural environments to assess and understand privacy awareness from multiple angles. It integrates four key factors: individual, technological, organizational, and social, to provide a complete picture of this complex concept. To empirically validate this framework, this study applies it to a case study of Saudi e-commerce users, aiming to answer the following research question: RQ: What is the current level of privacy awareness among Saudi e-commerce users?

By answering this question, this study contributes to the existing literature by:

- Introducing the Comprehensive Privacy Awareness Framework (CPAF) as a new and flexible framework for investigating, understanding, and assessing the complexity of privacy awareness in different contexts.
- Providing a complete and detailed assessment of privacy awareness among Saudi e-commerce users within this understudied context. This includes identifying specific knowledge and behavior gaps across individual, technological, organizational, and social dimensions.
- Developing recommendations that address both global and Saudi-specific needs to enhance privacy awareness among users.

2. Background and Literature Review

2.1. Understanding Privacy

Privacy is a complex and multifaceted issue [26]; it is also a fundamental right that protects individuals from the misuse of their personal information [1]. With the advancement of society and technology, privacy has developed from being a personal right and a desire to a legally recognized right in several nations, including Saudi Arabia. In 2021, Saudi Arabia issued the Personal Data Protection Law (PDPL), (<https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx>, accessed on 4 December 2025.) which aims to “protect the privacy of individuals and enable them to exercise their rights when their personal data is processed”. The PDPL applies to any entity processing the personal data of individuals residing in Saudi Arabia.

However, the exact meaning of privacy can differ significantly among individuals and even depends on the context. It has been discussed for centuries, and one of the earliest discussions on privacy can be traced back to Warren and Brandeis [27], who framed it as “the right to be left alone”. At present, with the advent of new technologies that collect and use personal information in unprecedented ways, defining privacy in our digital age has become even more complex.

Surrounding this, several key concepts are frequently discussed in the literature. One of the most critical is privacy awareness, which forms the foundation of our study.

2.2. Understanding Privacy Awareness

Privacy awareness is a critical factor shaping how individuals navigate digital environments. Researchers have proposed a variety of definitions to describe this concept. Some of these definitions are narrower and focus on specific aspects of privacy [15]. Others are more comprehensive, considering a wide range of factors [28]. One notable definition comes from Bergman in 2009 [7], who described privacy awareness as an individual’s understanding of a service provider’s privacy policies. Other studies have combined different definitions to cover more aspects. For example, the study [29] used Bergman’s 2009 definition [7], and the definition by Sim et al. [30], who described awareness as understanding the current state of information privacy, including data collection, use, and potential risks.

Nevertheless, privacy awareness remains challenging to define and measure consistently. One of the key issues is the lack of a unified conceptual and theoretical foundation. As discussed in previous studies [5,31], many researchers either fail to define “privacy awareness” clearly or conflate it with related concepts, such as knowledge, familiarity, or concerns. This leads to a fragmented understanding and inconsistent ways of measuring it across studies. Different studies measure privacy awareness in different ways, often focusing on specific factors, as will be discussed later. This fragmented approach makes it challenging to fully understand and measure the complexity of privacy awareness.

2.3. Scales and Key Influencing Factors in Privacy Awareness Research

As we explained earlier, privacy awareness has been studied and investigated from different angles, using different scales and by focusing on several factors. In this domain, several scales have been introduced; however, they typically focus on privacy concerns rather than directly measuring privacy awareness. For instance, the Concern for Information Privacy (CFIP) scale [32], which focuses on four dimensions for measuring privacy concerns (unauthorized access, errors, secondary use, and collection), is one of the oldest scales in this field. This was followed by the development of the Internet User Information Privacy Concerns (IUIPC) scale in 2004 [33], which consists of three dimensions: collection, control, and awareness of privacy practices. The Privacy Consciousness Scale (PCS) [34], which focuses on public consciousness and behaviors to do with individual privacy and others, was introduced in 2014. Additionally, there was the development of the Online Privacy Literacy Scale (OPLIS) in 2015 [35], which consists of five dimensions, including technical and legal knowledge.

While acknowledging their contributions, these scales have certain limitations. For example, the PCS does not take into account critical factors, such as data breach risks and security practices. The OPLIS scale also includes technical questions that may be difficult for non-technical users. Furthermore, the IUIPC scale does not address contextual factors, such as incentives offered.

Additionally, many studies define their own factors to assess privacy awareness rather than relying solely on these standardized measures, which confirms the complexity of this concept. One important factor that has been studied and found to influence awareness is understanding the benefits and risks of sharing information online, often known as privacy calculus [8,9,36]. Although benefits and risks were not clearly identified in previous scales, they have been extensively studied in the literature. In addition, an individuals’ awareness of privacy policies has been shown to directly impact privacy awareness [8,37–39]. Despite the importance of knowing the data protection regulations that mandate the existence of these policies, few studies have considered this factor [40]. These two critical factors correspond to what is measured in the OPLIS scale [35]. Another key factor that has been repeatedly studied is data control [8,38–41], which covers the ability to access and manage personal data. This factor aligns with what has been studied and directly measured in the IUIPC scale [33]. Some studies suggest that trust in online platforms can also influence individual privacy awareness [8,36,42].

2.4. Privacy Awareness Research in E-Commerce

Based on the above scales and factors, researchers have extensively studied privacy awareness in various fields since its emergence. These fields include social networks, the Internet of Things (IoT), and e-commerce. Focusing on e-commerce, studies have shown that privacy awareness and knowledge of security measures are major barriers to the sector’s growth. This lack of awareness can expose users to security risks, such as data breaches and the sharing of personal information without their knowledge or consent [4,5].

2.4.1. Privacy Awareness in Global E-Commerce

Global studies consistently reveal low levels of privacy awareness among e-commerce users. For instance, a study of Pakistani e-commerce users found a lack of understanding and awareness of privacy issues [17]. This supports the findings of another study conducted in the same region [43]. Similarly, research on South African e-commerce users confirmed these findings and found there to be a lack of awareness [44,45]. These studies underscore the critical need for education, awareness, and clear and concise privacy policies.

A study in China also observed a significant gap in privacy awareness among Chinese users [37]. Many users express concerns about potential privacy violations and have a limited understanding of privacy policies. Moving to India, a study found that security and privacy were the most important factors that affected the Indian users' confidence in e-commerce [46]. A study of U.S. and Brazilian consumers found that Americans consider their information to be more sensitive than consumers in Brazil and are less willing to share their information [47]. This indicates that American consumers have a higher level of privacy awareness compared to their Brazilian counterparts.

Focusing on European countries, a study shows a difference in the levels of awareness of cybersecurity in e-commerce between European countries [48]. Experts found that users are concerned about data sharing and payment security, which creates a barrier to online shopping. A Croatian study confirms this concern, as it found that privacy concerns negatively impact user behavior and purchasing decisions [49].

These findings are consistent with those of an Indonesian study [13] that found that a small but significant group of participants valued transparency and expressed privacy concerns. Another study in the region found that individuals with greater privacy awareness, online experiences, and a preference for robust privacy controls are more likely to express privacy concerns [40].

A Nigerian study found that most Nigerian users lack awareness of online privacy protection [50]. In addition, it was observed that very few participants read privacy policies due to their length and complexity.

2.4.2. Privacy Awareness in Saudi E-Commerce

Despite the rapid growth of e-commerce, research on privacy awareness among Saudi users remains limited compared to global research [16]. One early study on personal data sharing showed that Saudi customers are willing to share personal information online if they perceive clear benefits, such as discounts or exclusive product access. However, they remain hesitant when privacy concerns arise [51].

Similarly, in the context of social commerce, a study shows that privacy concerns influence users' attitudes toward information sharing and participation [38]. Many participants consider privacy policies necessary to minimize perceived risks. However, users often struggle to understand these policies. In the same year, researchers delved deeper into the effect of gender on privacy concerns in social commerce [39]. This study revealed that women place greater importance on different aspects of privacy and are more hesitant to share personal information online, especially when they perceive there to be inadequate privacy protection. This contrasts with an earlier study that found no significant difference in privacy concerns between genders [49]. Additionally, in the specific domain of mobile commerce, another Saudi study noted relatively low levels of security perception among Saudi users of mobile shopping applications [16].

2.4.3. Summary of Existing Literature and Gaps

These global and regional studies, despite their valuable insights, often focus primarily on privacy concerns or partial aspects of privacy awareness, or treat awareness as a

component of concern. It is crucial to distinguish between privacy awareness and privacy concerns. While privacy concerns represent “feelings and concerns when information is collected and used by entities for purposes and in ways that the individual did not intend [52]”, privacy awareness is defined more comprehensively as explained previously. Privacy awareness generally is conceptualized as an individual’s understanding of the current state of information privacy, including data collection, use, and potential risks, and the application of methods and practices to protect this privacy [5].

Furthermore, existing studies often rely on fixed scales (such as CFIP, IUIPC, and OPLIS) that produce a single numerical score for privacy awareness or often examine factors affecting this awareness in isolation. These studies fail to integrate social influences or distinguish between government regulations (e.g., PDPL) and privacy policies. Additionally, local research often neglects these specific regulatory (e.g., PDPL) and social dimensions within the Saudi context.

These gaps underscore the need for a comprehensive framework, which reconceptualizes privacy awareness as a standalone, multidimensional construct that integrates different factors such as individual, technological, organizational, and social dimensions into a single assessment logic.

3. The Comprehensive Privacy Awareness Framework (CPAF)

The above literature review reveals that, although existing scales, such as IUIPC and OPLIS, and related studies offer multidimensional perspectives, they frequently conflate distinct constructs, including privacy awareness, concern, and literacy, as discussed in the literature [5,31]. Furthermore, they tend to overlook and underestimate certain important factors or examine factors in isolation.

To address these research gaps, this study introduces the Comprehensive Privacy Awareness Framework (CPAF). The CPAF is a novel, multidimensional framework designed to understand and guide the assessment of individuals’ privacy awareness.

The framework aids in creating tools, such as questionnaires, to comprehensively and accurately assess users’ privacy awareness by asking questions about what users know (e.g., “Are you aware of the PDPL?”, “What security measures do you apply?”) rather than only relying on what they fear (e.g., “I worry about data misuse”). This approach ensures the identification of existing gaps in knowledge and behavior from different angles or dimensions. The framework offers a clear starting point, making it easier to track changes in awareness and provide evidence and recommendations.

This framework allows us to see privacy awareness as a multidimensional construct. It was developed through a review of the literature and the identification of the most frequently occurring important factors shaping individual privacy awareness and behavior. The CPAF is grounded in the Antecedents, Privacy Concerns, and Outcomes (APCO) model introduced by Smith et al. [53], which structures the relationships between causal factors, privacy perceptions, and behavioral outcomes. The APCO model was selected as the core theory using the IMPACT framework [54]. This approach ensures that the theory aligns closely with the research objectives and explains privacy awareness in the simplest and most effective way.

Within this framework, four main factors (individual, technological, organizational, and social) are identified as antecedents. Together, these factors shape and build an individual’s comprehensive privacy awareness, which then motivates behaviors that protect privacy. This structure is complemented by two theories: the Theory of Planned Behavior (TPB) [55], and Privacy Calculus Theory [56]. These theories aim to understand and predict human behavior concerning privacy issues and actions.

As shown in Figure 3, the framework categorizes these factors into four main categories: individual, organizational, technological, and social. These factors are classified based on their nature and source of influence. This categorization ensures covering and seeing privacy awareness from all angles without overlooking any factors that may affect said awareness. Additionally, it allows researchers to customize and select appropriate components based on their specific context or target population.

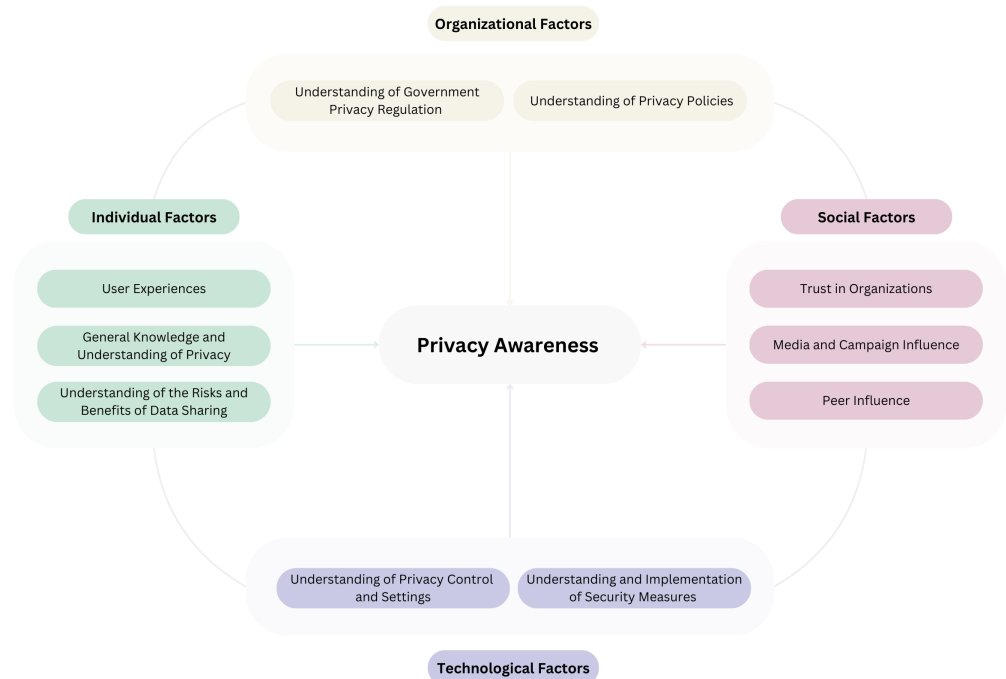


Figure 3. The Comprehensive Privacy Awareness Framework (CPAF).

3.1. Individual Factors

One of the most important aspects that researchers consider when studying human behavior is individual factors. These factors refer to the different personal characteristics, experiences, and basic knowledge that shape an individual's understanding, awareness, and behavior regarding privacy [57]. This factor will cover three sub-factors:

- **User Experience:** Positive and negative experiences directly shape and influence an individuals' awareness, opinions, and expectations regarding privacy. It can be considered part of the Antecedents in the APCO model (previous experiences contribute to privacy concerns) [37,40–42,49,58–61].
- **General Knowledge and Understanding of Privacy:** User privacy awareness begins with knowledge of general privacy concepts. A strong understanding enables individuals to interact more carefully with online platforms [14,62].
- **Understanding of Risks and Benefits:** Grounded in Privacy Calculus Theory, this factor describes how individuals weigh the expected benefits against the risks before disclosing their personal data. Research indicates that this awareness directly shapes behavior, where users tend to share more when perceiving benefits and less when they are aware of potential risks [14,56,63].

Based on the TPB theory, such factors are fundamental to how an individual perceives privacy and decides to protect it [64].

3.2. Technological Factors

According to [65,66], technology influences people's understanding of privacy. Consequently, studying and understanding technological aspects is essential. With the widespread use of the Internet and the massive amount of data exchanged, it is important to understand how we can control and protect our data. Therefore, two sub-factors are covered:

- **Understanding and Use of Personal Privacy Controls and Settings:** Being aware of available privacy options allows users to make better choices about how their data is shared and used. Users with stronger privacy management skills are less likely to engage in risky privacy behaviors [10,13,15,17,33,40,67,68]. Here, "awareness of personal privacy controls" and "awareness and use of privacy settings" are combined into one factor to link knowledge with practical application. This includes understanding their function and knowing how to access and modify them.
- **Understanding and Implementation of Security Measures:** Being aware of and applying security practices, such as using strong passwords and secure networks, is essential in today's digital life. The more security layers individuals apply, the harder it is for attackers to breach their data [45,67].

Based on the TPB theory, such factors may show an individual's ability and confidence when protecting their privacy using the available tools [69].

3.3. Organizational Factors

The awareness of the regulations and policies that are implemented and operated by organizations that deal with individuals' data is critical. According to the APCO model [61], a lack of awareness about these practices, especially when data is used without the users' knowledge, increases their concerns. Therefore, this factor will cover two sub-factors:

- **Understanding of Government Privacy Regulations:** Awareness of government data privacy laws (e.g., Saudi Arabia's PDPL) helps individuals understand their rights and request access, correct, or object to data processing [10,12,40–42,70].
- **Understanding of Privacy Policies:** Awareness and understanding of privacy policies enable individuals to make informed decisions regarding data sharing. These policies outline how personal data is collected, used, and stored by organizations [8,10,29,38].

While some studies treat the above aspects as one, it's important to distinguish between them. Government regulations (e.g., GDPR, PDPL) set the overall legal framework, while privacy policies serve as tools for organizations to document compliance and inform individuals about their data practices.

3.4. Social Factors

In the previous factors, the focus was primarily on the individual. However, it is also important to consider the broader context by examining the community surrounding the individual. People often follow the behavior of those around them, especially close contacts such as family and friends. Therefore, three sub-factors are covered:

- **Peer Influence:** Privacy-related behaviors can spread between individuals within a social network. Individuals are often influenced by their peers to determine what is considered normal or acceptable behavior. Based on the TPB theory, this may represent the "subjective norm," meaning what an individual perceives as acceptable or expected from others regarding privacy [64].
- **Media and Campaign Influence:** Media and campaigns related to privacy issues can significantly impact public knowledge and behavior. Further investigation is needed to explain how they contribute to raising the awareness of individual privacy [71,72].

- **Trust in Organizations and Platforms:** User trust in organizations and platforms plays a critical role in privacy-related behavior. It affects their willingness to share their data. Higher trust leads to more data disclosure, and a lack of trust will cause hesitation [15,18,61,63,69].

Although the effect of friends and community on an individuals' comprehensive privacy awareness has not been widely studied in the field of privacy awareness, it plays a significant role in shaping it [61,64,73].

3.5. Framework Contribution and Comparative Analysis

As illustrated in Figure 4 and Table 1, the CPAF integrates these factors to define and assess privacy awareness comprehensively. By combining these key factors into a unified structure, the framework overcomes the limitations of previous studies that often examined these aspects in isolation.

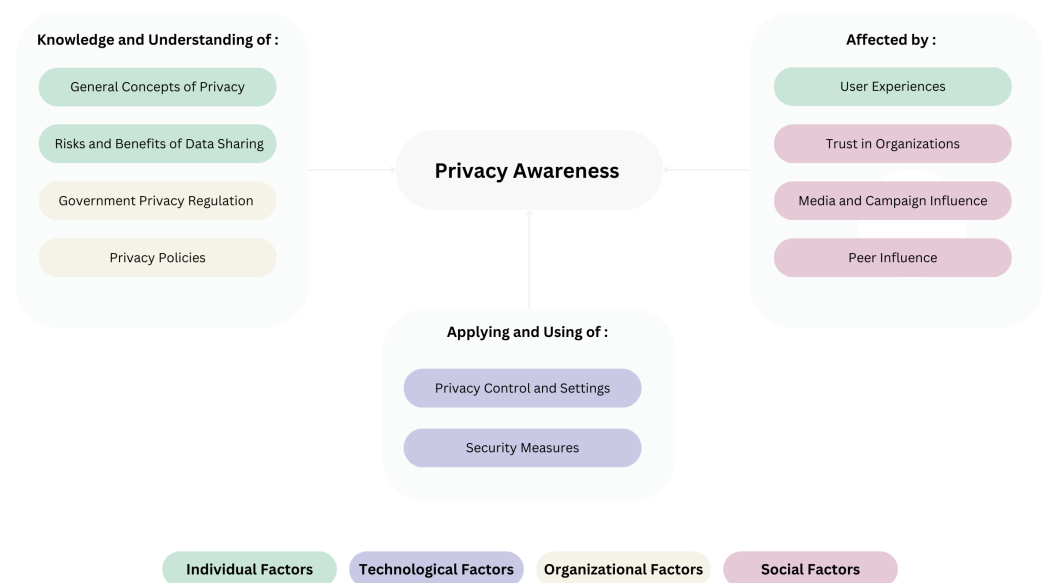


Figure 4. Components of Privacy Awareness According to the CPAF Framework.

Table 1. Summary of Factor Definitions.

Factors	Sub-Factors	Definition
Individual Factors	User Experience; General Knowledge; Risk–Benefit Understanding	Individual's personal knowledge, experiences regarding privacy
Technological Factors	Privacy Controls & Settings; Security Measures	Individual's knowledge of and capability to use available privacy and security tools
Organizational Factors	Government Regulations; Privacy Policies	Individual's understanding of legal rights and privacy policy
Social Factors	Peer Influence; Media Influence; Trust	Influence of the social environment.

Although the CPAF framework is based on the dimensions derived from existing measurement tools such as CFIP [32], IUIPC [33], and OPLIS [35], it reframes them within a more comprehensive perspective. It utilizes concepts such as data collection mechanisms, control, and legal knowledge, and integrates them into a comprehensive framework that aims to understand privacy awareness from all angles, rather than from a single perspective (Table 2).

Table 2. Comparison of CPAF and Established Privacy Scales.

Feature	CFIP (1996) [32]	IUIPC (2004) [33]	OPLIS (2015) [35]	CPAF
Type	Measurement scale	Measurement scale	Measurement scale	Conceptual framework
Output	Numerical score	Numerical score	Numerical score	Structured understanding
Primary Focus	Privacy concerns	Online privacy concerns	Privacy literacy	Comprehensive awareness
Main Dimensions	4 dimensions	3 dimensions	5 dimensions	4 main factors (10 sub-factors)
Core Coverage	Unauthorized access, errors, secondary use, collection	Collection, control, awareness of practices	Technical/legal knowledge, strategies, data protection	Individual, technological, organizational, social factors
Social Factors	Not included	Not included	Not included	Included
Regulatory Awareness	Not addressed	Limited	General legal knowledge	Distinguished (regulations vs. policies)

The CPAF distinguishes itself through three key features. Unlike previous studies, which have mostly focused on individual concerns or technical practices, the CPAF integrates social factors. Although the literature acknowledges the importance of these factors, they remain neglected in existing frameworks [61,64]. Additionally, the framework clearly differentiates between government regulations (e.g., PDPL, GDPR) and privacy policies. This separation allows for a better understanding of how these factors independently influence privacy awareness. Importantly, the CPAF is designed with the flexibility to suit different domains and contexts. It is adaptable to the continuous developments in digital tools, to updates in regulations and data protection laws, and to the changing expectations and values of society. This enables researchers and policymakers to apply it to different cultural, regulatory, and technological environments.

4. Methodology

This study employs a quantitative research design to empirically validate the proposed framework (CPAF) through a questionnaire. Specifically, the study selects the Saudi e-commerce sector as the empirical context to demonstrate the framework's practical application and effectiveness. As discussed earlier, this context was chosen due to the rapid and remarkable growth of the e-commerce sector in the Kingdom, in addition to the limited comprehensive research available on user privacy awareness in this field. Consequently, applying the CPAF offers an in-depth assessment of privacy awareness gaps among Saudi users.

4.1. Questionnaire Design and Validation

The questionnaire was developed based on the CPAF and included multiple items designed to cover each of the framework's factors (Individual, Technological, Organizational, and Social). Direct, scenario-based, and indirect questions were used. All questions were written in simple and clear Arabic, avoiding complex technical terms.

To ensure validity, the questionnaire items were evaluated by consulting experts and target participants. Initially, experts in statistics, security, privacy, and the Arabic language reviewed the questionnaire. Participants from the target population, representing different regions in Saudi Arabia, as well as a range of genders, education levels, and ages, provided their feedback. As a result, the questionnaire was refined to include 44 questions. The final version of the study questionnaire is provided in the Supplementary Materials (Questionnaire S1).

4.2. Data Collection

The questionnaire was reviewed by the Deanship of Graduate Studies at King Abdulaziz University. Following this review and approval, the questionnaire, designed using Microsoft Forms, was distributed through email and on social media platforms. The data collection process lasted for 40 days. Non-Saudi participants and those who did not use e-commerce platforms or did not agree to participate in the study were excluded, resulting in a final sample of 400 participants. This size is sufficient and statistically representative as it exceeds the minimum threshold set by Cochran's equation for large populations, which states that a sample of 384 participants is sufficient to achieve a 95% confidence level with a 5% margin of error [74].

5. Results and Discussion

5.1. Demographic Data

The demographic characteristics of the participants showed a balanced gender distribution, with 51.50% males and 48.50% females (Figure 5a). The majority of the participants were in the 25–34 age group (49.25%) (Figure 5b). In terms of educational level, most participants were highly educated, with 53.50% holding a bachelor's degree and 95 participants holding a postgraduate degree (Figure 5c). Finally, the Riyadh and Makkah regions had the highest representation, with 43.25% and 29.25%, respectively (Figure 5d).

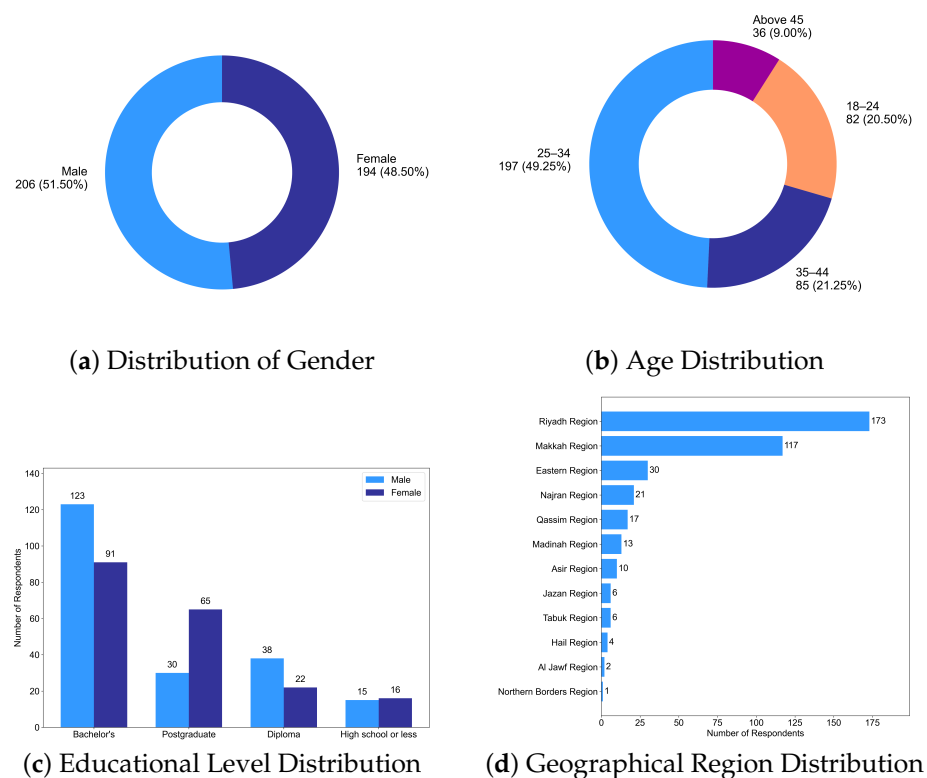


Figure 5. Demographic Distribution Overview (N = 400).

5.2. Structural Validation of the CPAF Framework

To ensure the integrity of the proposed framework, we used PLS-SEM with SmartPLS version 4. This analysis validates that the four factors of the CPAF (Individual, Technological, Organizational, and Social) are statistically associated and together represent a multidimensional structure.

As displayed in Table 3, the CPAF factors exhibit acceptable to strong outer loadings, ranging from 0.651 to 0.849. These loadings, along with the significant path coefficients

($p < 0.001$), validate that each factor makes a meaningful contribution to the overall assessment of privacy awareness. The VIF test showed values between 1.270 and 1.992. Since these numbers are much lower than the suggested limit of 5.0, it confirms that the factors are sufficiently distinct [75].

Table 3. Factor Loading, Weights, and VIF Values of the CPAF Framework.

Construct	Factor	Outer Loadings	Outer Weights	VIF
Privacy Awareness	Individual	0.725	0.339	1.555
	Organizational	0.651	0.339	1.270
	Social	0.729	0.339	1.349
	Technological	0.849	0.339	1.992

Note: Statistical significance for all weights and loadings is $p < 0.001$ based on 5000 bootstrap samples, as recommended by [75].

As illustrated in Figure 6, the path coefficients (β) from the four factors to privacy awareness were approximately equal and highly significant ($\beta \approx 0.339$, $p < 0.001$), which indicates a balanced contribution from each factor. The model achieved an R^2 value of 1.000, which is an expected result since the privacy awareness is defined using the four main factors; this R^2 value reflects a structural property of the formative two-stage PLS-SEM model rather than predictive power [75].

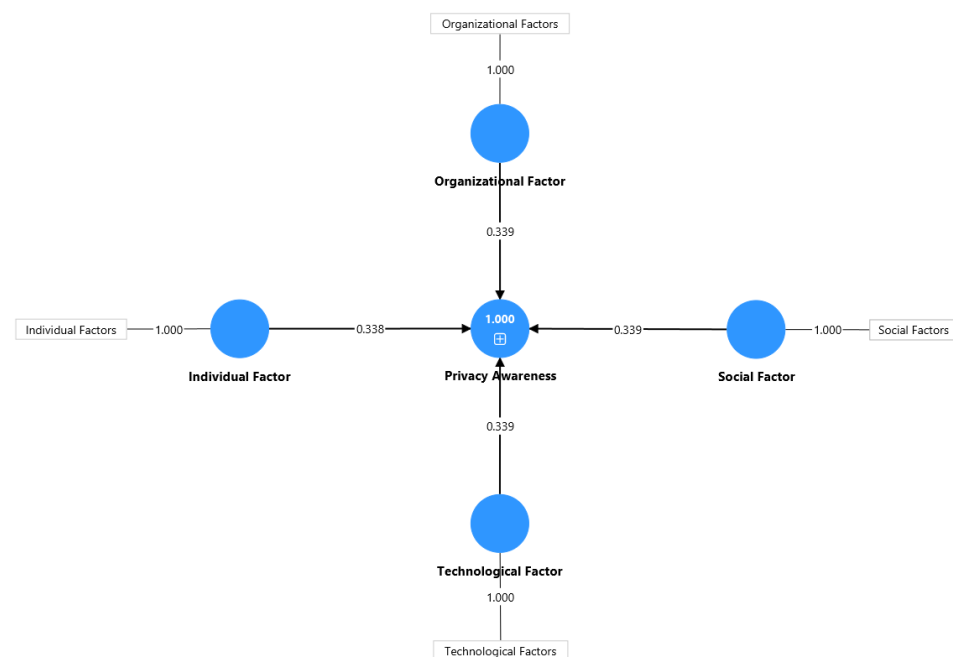


Figure 6. The CPAF Model with Path Coefficients.

5.3. Individual Factors

Starting with individual factors, it was found that 46 participants (11.50%) reported experiencing an online privacy violation (Figure 7). Notably, the chi-square test showed there to be a statistically significant relationship between experiencing a privacy violation and changing privacy settings ($\chi^2 = 11.44$, $p = 0.001$). Participants who experienced a privacy violation were significantly more likely to adjust their privacy settings than those who had not. Specifically, 47.83% of participants who experienced a breach changed their settings, compared to only 24.29% of those who did not experience a breach. However, the analysis revealed no statistically significant association between experiencing a privacy violation and key factors such as knowledge of how online stores collect data ($\chi^2 = 3.32$,

$p = 0.068$), or reading privacy policies before providing personal information ($\chi^2 = 1.21$, $p = 0.270$).

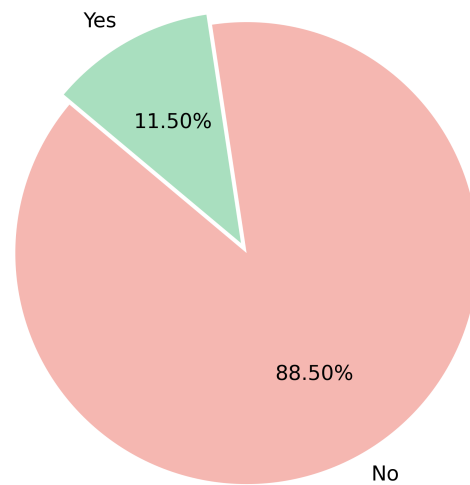


Figure 7. Experience of Privacy Violations Among Participants.

These findings are in line with those found in a study conducted in Croatia [49], where researchers found that previous negative experiences did not affect the level of interest and behaviors toward privacy protection. In contrast, another study observed that participants significantly changed their behaviors after experiencing privacy violations, and they began to read privacy policies more frequently [60]. These contrasting findings highlight the need for further research on the relationship between negative experiences, privacy awareness, and behavior.

Focusing on the basic concepts related to privacy, the majority of participants showed awareness of its meaning, and 90.25% strongly agreed on its importance ($Mean = 1.13$, $Median = 1.00$, $Std = 0.45$). However, when measuring the participants' awareness of data collection, 70.25% did not know how online stores collect and use their data (Figure 8 and Table 4). This observation confirms the findings reported in the literature across multiple domains [76]. This gap is concerning in today's digital environment. Data collection has become a common practice and is often done without obtaining direct approval from users [77]. This highlights the urgent need to improve individuals' understanding of privacy concepts and data collection methods to help them make informed decisions regarding their personal data.

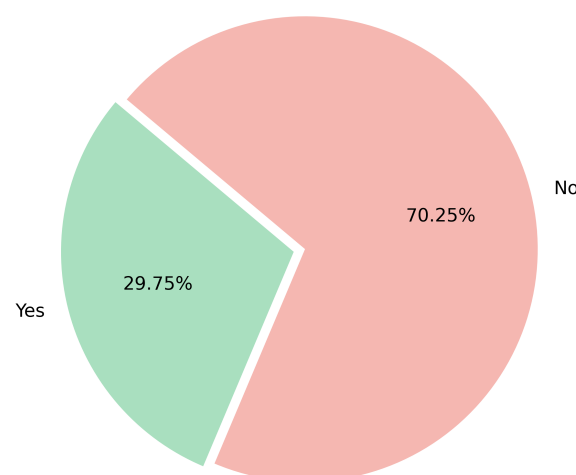


Figure 8. Percentage of Participants Aware of Data Collection Methods.

Table 4. Perceived Data Collection Methods Among Aware Participants (N = 119).

Method of Data Collection	Percent of Cases
Through purchases and payment information	69.75
Through tracking activity on websites and apps	75.63
Through cookies and other tracking technologies	69.75
Through social media account information (if linked)	54.62
Through voluntarily provided information (e.g., surveys)	41.18
Through purchasing information from third parties	36.97

When it comes to personal data, most of the participants were primarily concerned about sharing their national identity and bank card information (Table 5). This is consistent with what Nigerian shoppers thought in a 2017 study [50]. The majority of shoppers from both countries were concerned about sharing credit card data. Interestingly, it was also noted that their home address was one of the personal details that half of the Nigerian and Saudi participants did not prefer to share. This similarity reflects the shared concern between the two groups regarding the sensitivity of their home address and credit card information. Another interesting observation is that Saudi users expressed concern over sharing personal photos, with 335 respondents selecting the data as sensitive, while only 15.42% of the 220 Nigerian participants did the same.

Table 5. Participants' Perceptions of Sensitive Personal Information Types.

Category	Percent of Cases
Name	46.50
Identity Information	93.50
Email Address	51.00
Phone Number	54.00
Home Address	56.50
Bank Account and Card Numbers	89.75
License, Records, Personal Property Numbers	82.25
Personal Photos (Static and Motion)	83.75

By focusing more on the idea of balancing the benefits and risks of e-commerce, it is evident from Table 6 that product prices are the most significant factor influencing the choice of online stores for the majority of participants, followed by website security and a clear privacy policy. This information indicates that users prioritize competitive prices and recognize the importance of robust security and privacy policies. These findings align with a previous study conducted during the COVID-19 pandemic [78], which also highlighted the importance of product-related factors for Saudi users, such as product variety or price.

Table 6. Mean Ranks of Factors Influencing Online Shopping Decisions.

Option	Mean Rank
Product prices	2.29
Website security	2.79
Clarity of the company's privacy policies	2.92
Available payment options	3.70
Customer reviews and ratings	3.75
Website design	5.56

5.4. Technical Factors

From a technical perspective, while most participants recognized the importance of accessing and managing their personal data (*Mean* = 1.55, *Median* = 1.00, *Std* = 0.83), 73.00% had not recently updated their privacy settings, as illustrated in Figure 9b. Interestingly, a statistically significant relationship between updating privacy settings and not taking any security measures was confirmed using the chi-square test ($\chi^2 = 13.13$, $p < 0.001$). The results suggest that individuals who do not update their privacy settings are significantly more likely to take no security measures when shopping online. Specifically, 26.03% of those who did not change their settings reported taking no security measures compared to only 9.26% of those who updated their privacy settings.

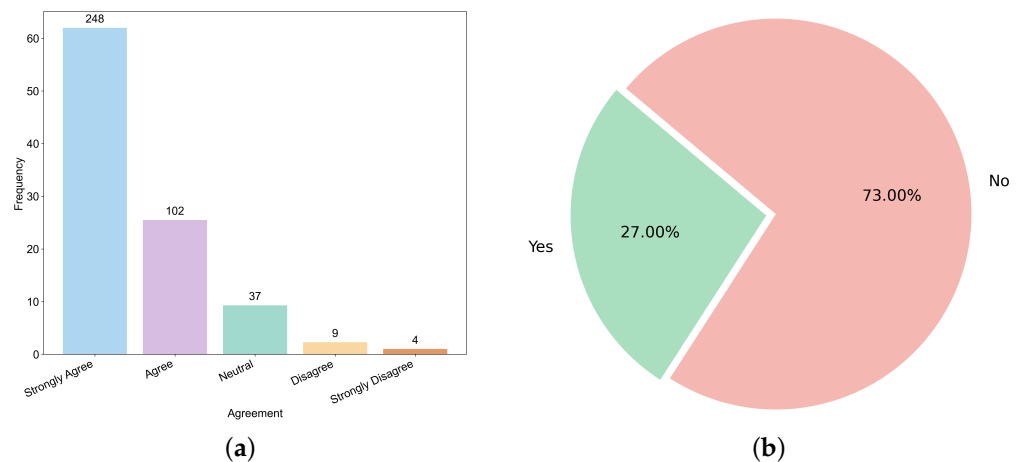


Figure 9. The Right to Access and Control Personal Data. (a) Agreement on the Right to Access, Control, and Correct Personal Data Held by Online Stores. (b) Changing Privacy Settings at Online Stores Recently.

Additionally, the findings showed that the main obstacles to changing these settings are their complexity and difficulty in understanding them. Specifically, 74.44% of the participants reported difficulty understanding the settings, and 69.26% found the process to be too complex or time-consuming. This observation aligns with the existing literature across multiple domains. Many users struggle with the complexity and inaccessibility of privacy settings [79]. Some researchers have suggested that the difficulty of using these settings is due to their poor design. It has been argued that presenting many options and settings in a single table may overwhelm users with a large amount of information to process [80]. This highlights the need for website and app designers across different sectors to simplify interfaces and privacy settings to encourage users to take more steps to protect their data.

Focusing on security measures, as can be seen in Table 7, 70.75% (283) of participants avoided opening unknown links or attachments, and 69.25% (277) avoided saving payment information. This result indicates a significant awareness of basic security practices. However, the use of advanced technologies, such as virtual private networks (VPNs) and two-factor authentication is still low. This finding suggests the need to raise awareness of the importance of these advanced measures to protect personal data. Compared to the study that focused on Nigerian shoppers [50], users from both countries agree on using specific security measures, such as deleting cookies and using antivirus software. However, it is worth noting that only 21.50% (89) of participants in this study report taking no security measures, unlike the Nigerian study, where 64.65% of participants (approximately 142 participants) admitted to not knowing or taking any security measures, although the number of participants in that study was 220 in total.

Table 7. Security Measures Taken by Participants.

Security Measure	Percent of Cases
No Action Taken	21.50
Clear Browsing History and Cookies	54.00
Use Strong Passwords and Change Them Regularly	64.25
Change Default Settings	40.75
Avoid Using Unsecured Public Wi-Fi	67.25
Use Incognito Browser	39.50
Use VPN	33.25
Use Two-Factor Authentication	46.75
Avoid Saving Payment Information	69.25
Use Antivirus Software	40.50
Block Pop-Ups	53.75
Backup Data	37.50
Verify No Sharing of Personal Data with Third Parties	57.75
Avoid Opening Unknown Links or Attachments	70.75
Check App Permissions	50.00
Use Regularly Updated Software	49.00
Avoid Installing Apps from Unknown Sources	67.75

By focusing on one of the most essential technologies for protecting information online, especially during online shopping, our study showed that participants differ in how they understand Secure Sockets Layer (SSL) certificates (and the padlock symbol that often represents them) (Figure 10). Although 45.50% of the participants never check for an SSL certificate before entering their personal information (Figure 10a), 45.25% consider its absence to be a critical factor in purchase decisions (Figure 10b). This finding highlights the lack of awareness of the importance of this fundamental technology. This lack of understanding is supported by a previous study [81], which found that users often misinterpret the padlock icon, and some even avoid transactions when it's absent. Interestingly, our study also found a correlation between SSL verification and other factors that influence online purchase decisions. A positive correlation was observed between SSL verification and website security ($\rho = 0.23$, $p < 0.001$). This result suggests that users who verify SSL prioritize website security when choosing shopping sites.

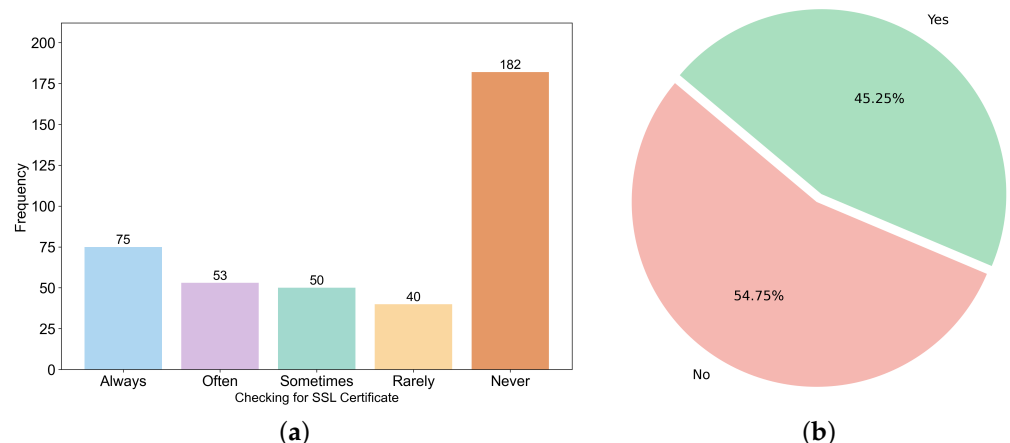


Figure 10. Impact of SSL Certificate Presence on Consumer Behavior During Online Shopping. (a) Frequency of Checking for SSL Certificate Before Providing Personal Information. (b) Influence of the Absence of an SSL Certificate on Participants' Purchasing Decisions.

5.5. Organizational Factors

This study found there to be a positive and strong correlation between knowledge of the Personal Data Protection Law (PDPL) and awareness of the Ministry of Commerce's regulations ($\rho = 0.79$, $p < 0.001$). This strong correlation indicates that individuals who are familiar with one set of regulations are likely to be knowledgeable about the other. However, as can be seen in Figure 11, 54.00% of participants reported being unaware of the Personal Data Protection Law in Saudi Arabia, and 43.75% were unaware of the Ministry of Commerce's regulations. This observation aligns with the findings of [37], which identified a similar lack of awareness of privacy laws among participants in China.

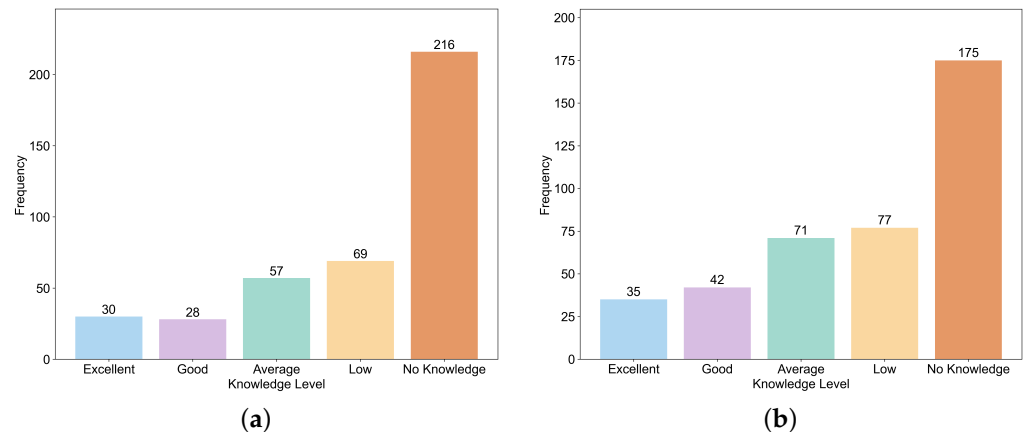


Figure 11. Participant Awareness of Privacy Laws and E-Commerce Regulations. (a) Awareness of the Personal Data Protection Law (PDPL). (b) Awareness of Saudi E-Commerce Regulations.

Interestingly, the results revealed a statistically significant association between the awareness of privacy regulations (PDPL and Ministry of Commerce's regulations) and the likelihood of reporting uncertainty about what actions to take during a data breach (χ^2 ranging from 22.96 to 23.14, ρ ranging from 0.23 to 0.24, $p < 0.001$). Participants with lower awareness were more likely to report not knowing what actions to take when faced with a potential data breach. This finding highlights the critical role of awareness in empowering individuals to take appropriate actions during such events.

When it comes to privacy policies, 68.00% of our participants reported not reading privacy policies before submitting their personal information (Figure 12a). These results are similar to many other studies in different fields. A study in China found that few participants read privacy policies [37]. Similarly, studies in Croatia, Indonesia, and Pakistan revealed that the majority of their participants do not read policies due to their length and complexity [17,49,82]. This finding confirms that many users often do not read privacy policies when engaging in e-commerce, perhaps due to their length and the complex technical terms used. Yet, individuals in our study showed a willingness to read policies if there are clear summaries, as illustrated in Figure 12b. This finding highlights the need to simplify privacy policies for better readability and understanding.

5.6. Social Factors

Focusing on the social factors and the environment surrounding the participants, it was observed that the level of trust users have in the ability of online stores to protect their personal data is generally low (Figure 13a). Only 35.50% have moderate trust, and 34.00% have no trust at all. This suggests that users have doubts and concerns about the security of their data when dealing with online stores. Additionally, the results reveal a strong and highly significant correlation between the level of trust in e-commerce stores' ability to protect personal data and the belief that trust influences the willingness to share personal

information ($\rho = 0.56$, $\chi^2 = 187.86$, $p < 0.001$). In simple terms, the higher the trust users have in online stores, the more likely they are to believe that this trust influences their decision to share personal information. This finding is in line with research suggesting that trust significantly influences an individuals' willingness to disclose personal information online [18,83].

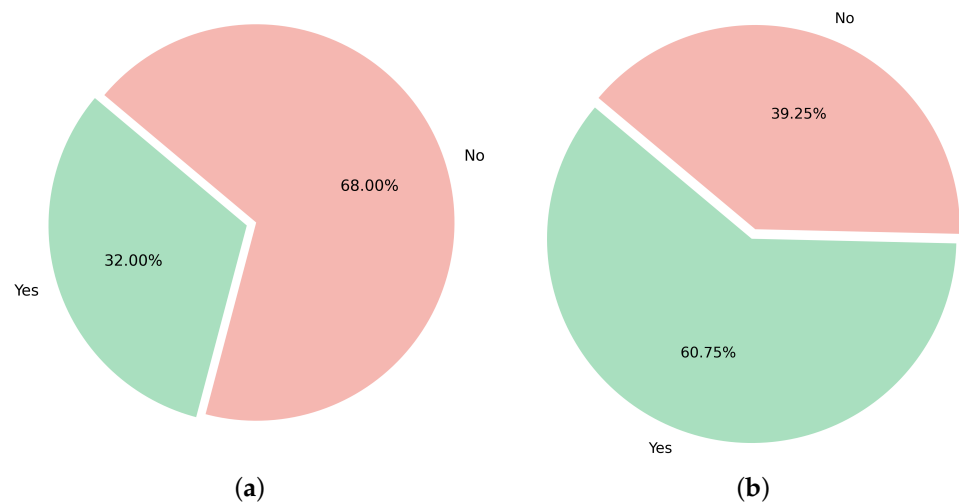


Figure 12. Awareness and Reading of Privacy Policies. (a) Reading Privacy Policies Before Submitting Personal Information. (b) Would Clear Summaries Encourage Reading Privacy Policies?

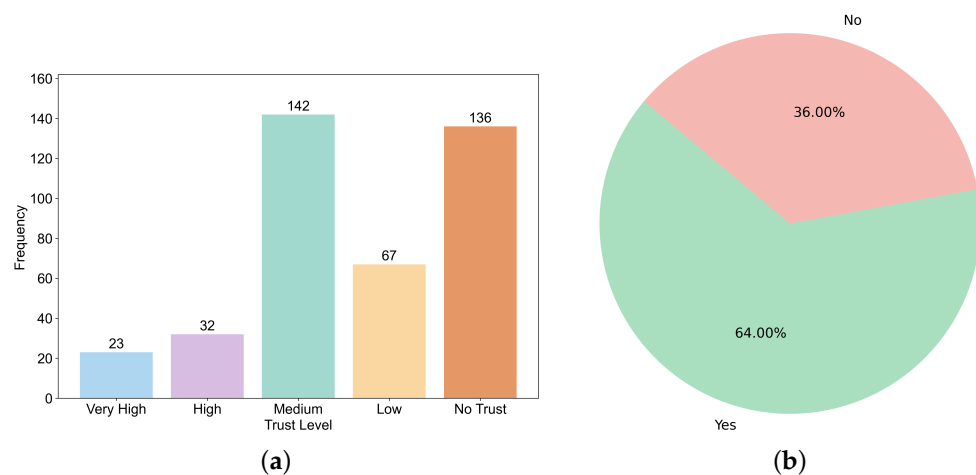


Figure 13. Trust in Online Platforms. (a) Participants' Trust in Online Stores' Ability to Protect Their Personal Data. (b) Impact of Trust on Willingness to Share Personal Information.

When it comes to following the news and the impact of campaigns, Figure 14a shows that the majority of participants do not follow news related to data breaches. Meanwhile, government campaigns related to security and privacy influenced 56.50% of the participants (Figure 14b). As shown in Table 8, the results of the chi-square test showed statistically significant values ($p < 0.001$) between being influenced by government campaigns and awareness of privacy concepts, changing privacy settings, and reading privacy policies. This means that individuals who reported that government campaigns influenced their interactions with online stores were more familiar with the concept of "privacy" and were more likely to change their privacy settings in online stores and even read privacy policies before providing personal information.

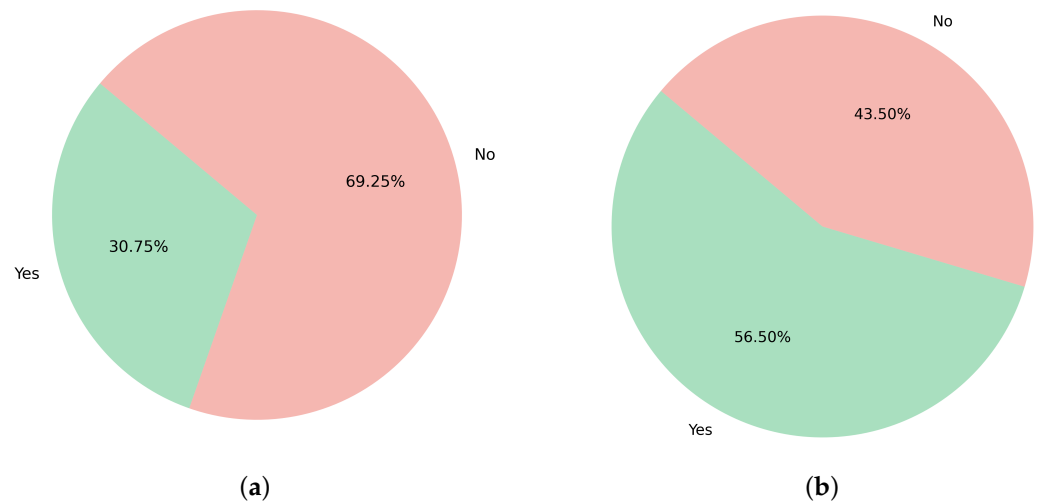


Figure 14. Following News and Government Campaigns Impact. (a) Participants' Interest in Following News About Data Breaches or Privacy Issues. (b) Impact of Government Campaigns on Users' Behavior Toward E-Commerce Security and Privacy.

Table 8. Relationship Between Government Campaigns and Behavioral Changes Due to Negative Experiences with Key Factors.

Factor	Government Campaigns				Behavioral Changes			
	Yes	No	χ^2	p -Value	Yes	No	χ^2	p -Value
Awareness of Privacy Concept	183	51	108.08	< 0.001	188	46	120.39	< 0.001
Change Privacy Settings	87	21	34.83	< 0.001	90	18	40.40	< 0.001
Read Privacy Policies	109	19	62.89	< 0.001	111	17	65.76	< 0.001

Note: χ^2 = Pearson Chi-Square. Significant at $p < 0.05$.

These findings confirm that campaigns focused on privacy and security can contribute to enhancing an individuals' understanding of privacy issues and improving their security behaviors. This is consistent with previous studies [71,72], which have shown that such awareness campaigns can influence user behavior and serve as important wake-up calls. Therefore, it is recommended to enhance security campaigns and encourage companies to implement more effective security campaigns. Future campaigns should focus on providing clear information about the practical steps that individuals can take to protect themselves.

Focusing on social relationships, the results in Figure 15a showed that 75.75% of participants discussed their privacy concerns with their peers. In addition, 57.50% reported changing their behaviors in response to negative experiences shared by said peers (Figure 15b). This confirms that social relationships influence an individuals' behavior toward privacy and security. This pronounced social influence reflects the cultural specificity of Saudi society, which is characterized by its deeply interconnected nature [84]. This shows that practices related to privacy and digital security in Saudi Arabia are the result of social interaction and shared values, rather than just technical decisions made in isolation from the surrounding environment.

As shown in Table 8, the chi-square results revealed statistically significant values between changing behaviors based on negative experiences shared by peers and adopting security measures. For example, individuals who changed their behaviors after hearing negative experiences from their peers were more likely to change their privacy settings ($p < 0.001$), and even read privacy policies ($p < 0.001$). These findings suggest that negative experiences shared by peers can significantly influence individuals to adopt more secure online behaviors.

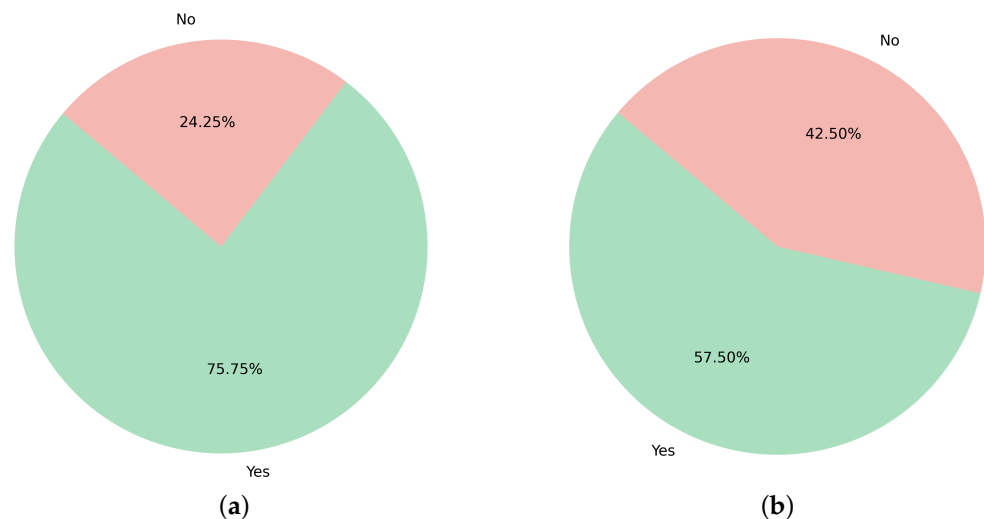


Figure 15. Influence of Relatives and Friends on Privacy Behavior. (a) Discussion of Privacy Concerns with Relatives and Friends. (b) Changes in Privacy Behavior After Hearing Negative Experiences from Relatives.

The results show that the majority of respondents (75.44%) rely on ratings and reviews to check the security of an online store before using it, even if it is recommended by a friend. This is followed by reviewing the app's permissions and privacy policy (58.15%). Although most participants reported that they do not read privacy news, 54.89% indicated here that they follow online reports or articles about recommended app security.

5.7. Investigating the Relationship Between Demographic Characteristics and Privacy Awareness

Previous research has revealed conflicting results on how demographic characteristics influence privacy awareness and concerns [17,39,49]. To address this gap, this section examines the impact of key demographic characteristics on privacy awareness, such as age, gender, and education. However, the unequal distribution of participants across cities, as shown in Figure 5d, led us to exclude the city from our analysis.

Based on the findings in Table 9, it is evident that demographic factors like gender, education, and age influence privacy awareness and behavior among individuals [17,39]. The results show that females are more aware of privacy concepts and read privacy policies. Meanwhile, males tend to take more security measures to protect themselves, such as using strong passwords, avoiding public Wi-Fi networks, and using antivirus software, in addition to being more aware of data protection laws and regulations.

Regarding education, individuals with higher education show greater awareness of privacy and more careful behavior, and they are more influenced by government campaigns and news related to data breaches.

When it comes to age, the 25–34 age group is considered to be the most aware and concerned with many factors, such as reading privacy policies, taking technical measures to protect themselves, being influenced by awareness campaigns, and discussing privacy issues with family and friends. The results show that the 18–24 age group is the most interested in following news related to data breaches.

Table 9. The Relationship between Demographic Characteristics and Privacy Awareness.

Factor	Description	Gender				Education				Age			
		Test	χ^2/Z	p	Conclusion	Test	χ^2/H	p	Conclusion	Test	χ^2/H	p	Conclusion
Individual	Awareness of privacy concept	χ^2	64.36	<0.001	Females more aware	χ^2	54.44	<0.001	Higher edu more aware	χ^2	52.19	<0.001	Age 25–34 more aware
	Experienced violation	χ^2	0.71	0.399	No diff.	χ^2	19.89	<0.001	Higher edu exp more	χ^2	2.76	0.431	No diff.
	Data collection aware.	χ^2	8.45	0.004	Females more aware	χ^2	23.45	<0.001	Higher edu more aware	χ^2	16.83	0.001	Age 25–34 more aware
	Website security	M-W	−2.72	0.006	Males more concern	K-W	2.24	0.525	No diff.	K-W	11.20	0.011	25–34 more concern
	Policy clarity	M-W	−8.19	<0.001	Females concern	K-W	64.03	<0.001	Higher edu concern	K-W	41.24	<0.001	25–34 more concern
Technical	Changed settings	χ^2	33.33	<0.001	Females more aware	χ^2	9.79	0.020	Higher edu more aware	χ^2	20.49	<0.001	Age 25–34 more aware
	Other measures	χ^2	Range	<0.05	Males more aware	χ^2	Range	<0.05	Higher edu more aware	χ^2	Range	<0.05	25–34 more aware
Organizational	Awareness of PDPL	M-W	−4.24	<0.001	Males more aware	K-W	9.29	0.026	Higher edu more aware	K-W	11.21	0.011	25–34 more aware
	Ministry regulations	M-W	−5.46	<0.001	Males more aware	K-W	5.49	0.140	No diff.	K-W	13.29	0.004	25–34 more aware
	Reading policies	χ^2	38.47	<0.001	Females more aware	χ^2	3.81	0.283	No diff.	χ^2	21.95	<0.001	Age 25–34 more aware
Social	Trust in online stores	M-W	−7.74	<0.001	Males more trust	K-W	33.79	<0.001	Higher edu more trust	K-W	86.59	<0.001	25–34 more trust
	Follow privacy news	χ^2	27.86	<0.001	Females follow news	χ^2	19.30	<0.001	Higher edu follow	χ^2	28.69	<0.001	18–24 follow news
	Campaigns behavior	χ^2	83.90	<0.001	Females more infl.	χ^2	42.79	<0.001	Higher edu more infl.	χ^2	45.64	<0.001	25–34 more infl.
	Discuss concerns	χ^2	12.19	<0.001	Males discuss more	χ^2	7.59	0.055	No diff.	χ^2	15.89	0.001	25–34 discuss more
	Relatives' exp.	χ^2	80.92	<0.001	Females more infl.	χ^2	44.38	<0.001	Higher edu more infl.	χ^2	35.45	<0.001	25–34 more infl.

Note: χ^2 = Pearson Chi-Square; M-W = Mann–Whitney U test (Z value); K-W = Kruskal–Wallis test (H value). $p < 0.05$ is significant; “No diff.” = No significant difference.

5.8. Key Findings

In summary, the results of this study confirm that privacy awareness is not a simple concept but a complex and multidimensional construct. As demonstrated through the CPAF framework, the individual, technical, organizational, and social factors are associated. Therefore, a user's overall privacy awareness cannot be represented by a single and unified degree that is simply "high" or "low". As shown in Table 10, an individual may show a high level of awareness in one factor (e.g., prioritizing website security as an important factor when choosing online stores) while simultaneously showing a low level in another (e.g., a lack of awareness of data collection practices). Similarly, a user might apply basic security awareness (e.g., avoiding unknown links) yet fail in another technological aspect (e.g., not updating privacy settings as reported by 73.00% of users). This study confirms that awareness and knowledge of one factor are significantly associated with other factors.

Figure 16 presents the characteristics of Saudi e-commerce users and summarizes their level of awareness across the factors. Despite the demographic differences, there are gaps remaining in the Saudi users' awareness of privacy. There are gaps in their understanding of data collection and security practices, as well as limited awareness of privacy regulations and policies. Furthermore, despite personal and social influences, users still need simpler education, tools, and solutions to deal with the current digital privacy challenges and increased awareness to overcome these gaps.

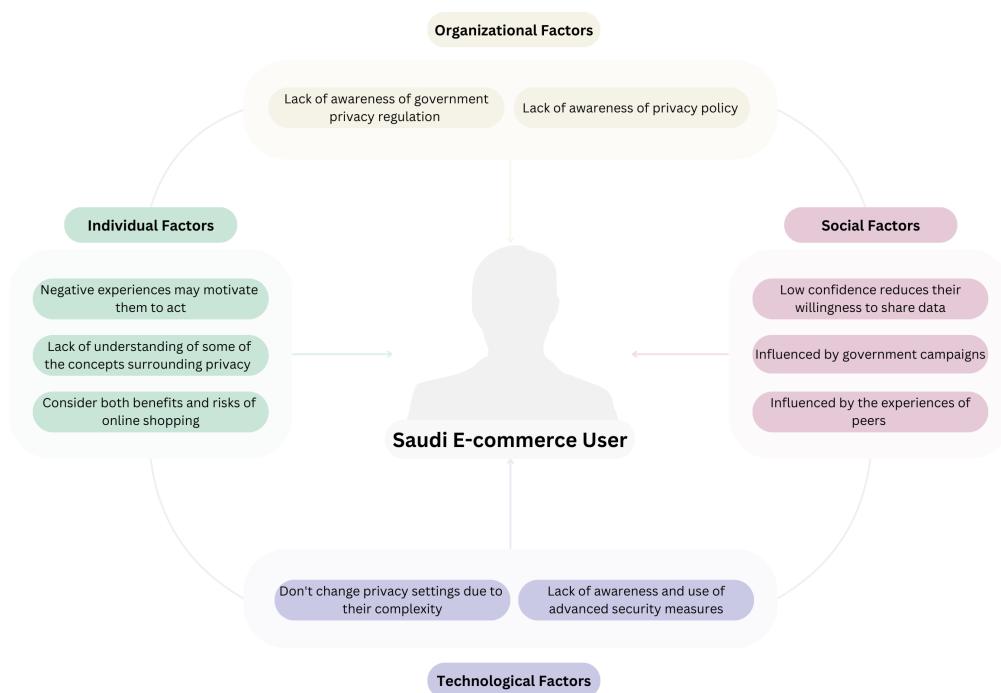


Figure 16. Characteristics of Saudi E-commerce Users Regarding Privacy Awareness Based on the CPAF Framework.

5.9. Targeted Recommendations

Based on the research findings, practical recommendations have been proposed and summarized in Table 11 to improve online privacy and security awareness. While these recommendations were developed in response to the specific challenges and needs we identified in our study among Saudi users (such as awareness of the PDPL), they are designed to be globally applicable (such as simplifying privacy policies and launching awareness campaigns).

Table 10. Summary of Key Study Findings.

Framework Factor	Key Finding	Statistical Evidence	Discussion
Individual Factors	11.50% experienced a privacy violation. Here, privacy violation experience affects setting changes but not knowledge of data collection or policy reading.	$p = 0.001$ (settings), $p = 0.068$ (collection knowledge), $p = 0.270$ (policy reading).	Negative experiences drive action, but do not automatically enhance knowledge or policy engagement.
	Basic awareness of privacy exists, but low awareness of data collection practices.	70.25% unaware of data collection.	This indicates a significant gap in understanding online data collection methods.
	Prioritize price, security, and clear privacy policies.	Product prices are rated the highest, followed by website security and privacy policy (as prioritized by participants).	Consumers perform a privacy calculus, balancing perceived benefits with potential risks.
Technological Factors	Most users had not recently updated their privacy settings, due to the complexity and difficulty in understanding them.	73.00% did not update settings, $p < 0.001$ with poor practices.	Strong correlation between not updating settings and poor security practices.
	Users show some basic security awareness, but often do not use advanced tools or understand key features like SSL certificates.	283 avoided unknown links, 277 avoided saving info, low VPN/2FA use, 45.50% ignore SSL, 45.25% see it as critical.	Basic security awareness is present, but advanced measures are not widely adopted.
Organizational Factors	Low regulatory awareness.	54.00% unaware of PDPL, 43.75% unaware of Ministry of Commerce (MoC) regulations.	This indicates a significant gap in user knowledge regarding data protection regulations and their rights.
	Users generally neglect privacy policies, but are willing to read them if clear summaries are provided.	68.00% do not read privacy policies, 60.75% willing to read them if summaries.	User engagement with privacy policies is low, but is influenced by policy summaries and awareness of relevant regulations.
Social Factors	Social relationships affect users' privacy and security behavior. Many participants discuss privacy with peers and adjust their actions based on others' experiences, particularly negative ones.	75.75% discuss, 57.50% change behavior, $p < 0.001$ with measures and policy reading.	Peer experiences promote awareness and encourage security practices.
	While campaigns positively influence behavior, most users do not actively follow news about breaches.	56.50% influenced by campaigns, $p < 0.001$ with awareness of privacy concepts and behavior.	This indicates a significant gap in users' ongoing awareness of privacy threats.
	Low organizational trust.	35.50% moderate trust, 34.00% no trust, $p < 0.001$ with willingness to share info.	Trust impacts privacy behavior and willingness to share data in e-commerce.

Table 11. Summary of Targeted Recommendations.

Category	Recommendation	Statistical Evidence	Justifications
Further Research	Explore how negative online experiences truly affect what users know and do about privacy.	Violation experience affects setting changes ($p = 0.001$) but not policy reading ($p = 0.270$) or collection knowledge ($p = 0.068$).	Our study found that bad experiences make users change settings, but do not always lead to more privacy knowledge or policy reading.
Education & Campaigns	Launch future targeted campaigns and programs to increase understanding of privacy basics, data collection practices, advanced security mechanisms (like VPNs, 2FA), key security technologies (like SSL certificates), and relevant government privacy laws (like PDPL) and Ministry of Commerce regulations. These campaigns should focus on providing clear, specific guidance on practical steps individuals can take to protect themselves.	70.25% unaware of data collection; 54.00% unaware of PDPL; 43.75% unaware of MoC regulations; 56.50% influenced by campaigns.	Our study showed that many participants were affected by the current government campaigns. These campaigns had a strong positive impact on the adoption of several security practices.
Social Influence	Using social media and peer influence to spread privacy awareness and promote safer online practices.	75.75% discuss privacy with peers; 57.50% change behavior after hearing peers' negative online experiences.	Our study showed that many participants were strongly influenced by their peers' negative online experiences. These experiences prompted them to adopt better privacy and security practices.
Simplified Design	Prioritize simplifying website and app designs, particularly their privacy settings. Encourage companies to develop privacy policies that include clear, easy-to-read summaries to improve readability and comprehension.	73.00% did not update settings due to complexity; 60.75% willing to read summaries of policies.	Our study showed that a significant number of participants are prevented from updating their privacy settings by the complexity and difficulty of understanding them. Most users do not read privacy policies, but they are willing to read them if they are presented in a summarized form.

6. Conclusions

This study has introduced the Comprehensive Privacy Awareness Framework (CPAF), a novel and adaptable framework suitable for different global contexts. This framework includes several factors surrounding privacy awareness, which make it a valuable tool for researchers in multiple fields. Researchers can effectively customize it to meet the unique needs of different populations, whether in e-commerce, social media, or other fields. For instance, researchers can modify the organizational and regulatory factors to reflect their local laws, such as the General Data Protection Regulation (GDPR) in Europe or the Personal Data Protection Law (PDPL) in Saudi Arabia. Similarly, social factors, which include peer influence and media campaigns, can be modified based on the cultural context. Additionally, technological factors can be adjusted to reflect the level of technological evolution in the region under study. This flexibility makes the framework effective for studying privacy awareness in various contexts.

This study applied and empirically validated the framework by investigating privacy awareness among Saudi e-commerce users. To the best of the authors' knowledge, this represents one of the first studies to investigate privacy awareness in the Saudi e-commerce context using a multi-dimensional framework. The results highlight significant gaps in Saudi users' knowledge and behavior, especially regarding data collection practices, privacy policy engagement, and the adoption of advanced security measures. Furthermore, the study confirmed the nature of privacy awareness as a multifaceted construct. It goes beyond

a simple theoretical concept to become an integrated system of knowledge, practices, and skills. Finally, based on our findings, we have offered practical recommendations to enhance online privacy and security awareness. By implementing these recommendations, e-commerce practitioners and policymakers can improve privacy awareness and promote safer online behaviors in the Saudi e-commerce sector and globally. The CPAF provides a universal tool for policymakers to identify specific privacy gaps and develop targeted, evidence-based strategies for safer digital environments.

Despite these contributions, certain methodological limitations should be considered. First, the use of non-probability sampling through digital channels (email and social media) may introduce a sample or systematic bias toward digitally active users. However, this approach may be justified as the study specifically targets e-commerce users who are naturally active in digital environments. Second, the voluntary nature of participation may create the possibility of self-selection bias. However, the study attempted to limit these effects by using filtering questions at the beginning of the questionnaire to ensure that it targeted actual e-commerce users in Saudi Arabia. In addition, as with most survey-based studies, although the instrument included some objective questions, it partially relied on self-reported data, which may introduce social desirability bias, whereby participants may overestimate their behaviors. This bias appears to be limited in the current study as substantial proportions of participants reported low awareness and limited protective behaviors, suggesting that they responded honestly rather than overstating their awareness or actions. Future studies should adopt probability sampling methods and expand data collection channels to include non-digital means.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/jtaer21020050/s1>, Questionnaire S1: Study survey instrument used for data collection.

Author Contributions: N.D.A.: Conceptualization, Methodology, Formal analysis, Investigation, Writing—Original Draft, Visualization. M.A.: Conceptualization, Writing—Review and Editing, Supervision, Project administration. M.B.: Conceptualization, Writing—Review and Editing, Supervision, Project administration. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and the research protocol was reviewed, approved, and distributed by the Deanship of Graduate Studies at King Abdulaziz University (approval code: 242620011; approval date: 16 July 2025).

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

Data Availability Statement: The data presented in this study are not available due to privacy restrictions and the assurance of confidentiality provided to participants.

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

References

1. Barth, S.; Ionita, D.; Hartel, P. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* **2022**, *55*, 63. [\[CrossRef\]](#)
2. Fiesler, C.; Hallinan, B. “We Are the Product”: Public Reactions to Online Data Sharing and Privacy Controversies in the Media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–13. [\[CrossRef\]](#)
3. Al-Alawi, A.I.; Mehrotra, A.A.; Elias, H.; Safdar, H.S.; Al-Bassam, S.A. The Implications of Unethical and Illegal Behavior in the World of E-Commerce. In *Ethical Consumerism and Comparative Studies Across Different Cultures: Emerging Research and Opportunities*; IGI Global: Hershey, PA, USA, 2020; pp. 152–230. [\[CrossRef\]](#)

4. Dey, K.; Mondal, P. Privacy awareness among the academic social network users. *Libr. Philos. Pract.* **2019**, 2905. Available online: <https://digitalcommons.unl.edu/libphilprac/2905> (accessed on 4 December 2025).
5. Soumelidou, A.; Tsohou, A. Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. *Telemat. Inform.* **2021**, *61*, 101592. [\[CrossRef\]](#)
6. Deuker, A. Addressing the Privacy Paradox by Expanded Privacy Awareness—The Example of Context-Aware Services. In *Privacy and Identity Management for Life*; Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 275–283.
7. Bergmann, M. Testing Privacy Awareness. In *Proceedings of the The Future of Identity in the Information Society*; Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 237–253.
8. Abdulatif, A.; Alturise, F. Awareness of data privacy on social networks by students at Qassim University. *Int. J. Adv. Comput. Res.* **2020**, *10*, 194–205. [\[CrossRef\]](#)
9. Ali, M.N.Y.; Rahman, M.L.; Jahan, I. Security and Privacy Awareness: A Survey for Smartphone User. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 483–488. [\[CrossRef\]](#)
10. Almutairi, O.; Almarhabi, K. Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 614–622. [\[CrossRef\]](#)
11. Aleisa, N.; Renaud, K.; Bongiovanni, I. The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Comput. Secur.* **2020**, *96*, 101897. [\[CrossRef\]](#)
12. Aleisa, N.; Renaud, K. Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions. In *Volume 1, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security IoTBDs, Porto, Portugal, 24–26 April 2017*; ScitePress: Porto, Portugal, 2017; pp. 198–205. [\[CrossRef\]](#)
13. Rusna, R. *Privacy Concerns of Indonesian Internet Users: Investigating the Level of Concern Among Ecommerce Users*; KTH Royal Institute of Technology: Stockholm, Sweden, 2022.
14. Lee, K.; Attablayo, P. Examining the Impacts of Privacy Awareness on User's Self-Disclosure on Social Media. Ph.D. Thesis, University of Cincinnati, Cincinnati, OH, USA, 2023.
15. Sah, J.; Jun, S. The Role of Consumers' Privacy Awareness in the Privacy Calculus for IoT Services. *Int. J. Hum.-Comput. Interact.* **2024**, *40*, 3173–3184. [\[CrossRef\]](#)
16. 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. [\[CrossRef\]](#)
17. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [\[CrossRef\]](#)
18. Al-Azzawi, G.A.; Miskon, S.; Abdullah, N.S.; Ali, N.M. Factors Influencing Customers' Trust in E-Commerce during COVID-19 Pandemic. In *Proceedings of the 2021 7th International Conference on Research and Innovation in Information Systems (ICRIIS)*, Johor Bahru, Malaysia, 25–26 October 2021; pp. 1–5. [\[CrossRef\]](#)
19. Ministry of Commerce. *Quarterly Business Sector Report Q3 2023*; Ministry of Commerce: Islamabad, Pakistan, 2023.
20. Riyadh Chamber. *E-Commerce in Saudi Arabia—Indicators and Numbers*; Riyadh Chamber: Riyadh, Saudi Arabia, 2021.
21. Saudi Central Bank (SAMA). *57th Annual Report*; SAMA: Riyadh, Saudi Arabia, 2021.
22. Communications, Space and Technology Commission. *Saudi Internet Report 2023*; Communications, Space and Technology Commission: Riyadh, Saudi Arabia, 2023.
23. Research and Information Center—Abha Chamber of Commerce. *E-Commerce Market Report in the Kingdom*; Research and Information Center—Abha Chamber of Commerce: Abha, Saudi Arabia, 2023.
24. Jeddah Chamber. *E-Commerce Statistics in the Kingdom of Saudi Arabia*; Jeddah Chamber: Riyadh, Saudi Arabia, 2020.
25. Monsha'at. *Unlocking E-Commerce: Thematic Report*; Monsha'at: Riyadh, Saudi Arabia, 2024.
26. Barth, S.; Ionita, D.; de Jong, M.D.T.; Hartel, P.H.; Junger, M. Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services. *IEEE Trans. Prof. Commun.* **2021**, *64*, 354–373. [\[CrossRef\]](#)
27. Warren, S.; Brandeis, L. The right to privacy. In *Killing the Messenger: 100 Years of Media Criticism*; Columbia University Press: Columbia, UK, 1989; pp. 1–21.
28. Arias, J.M. Privacy in the Context of Smart Home Environments: Based upon a Survey of Experts. Master's Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2014.
29. Soumelidou, A.; Tsohou, A. Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram. *Inf. Technol. People* **2019**, *33*, 502–534. [\[CrossRef\]](#)
30. Sim, I.; Liginlal, D.; Khansa, L. Information Privacy Situation Awareness: Construct and Validation. *J. Comput. Inf. Syst.* **2012**, *53*, 57–64.
31. Correia, J.; Compeau, D. Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hilton Waikoloa Village, HI, USA, 4–7 January 2017. [\[CrossRef\]](#)

32. Smith, H.J.; Milberg, S.J.; Burke, S.J. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Q.* **1996**, *20*, 167–196. [[CrossRef](#)]
33. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Info. Sys. Res.* **2004**, *15*, 336–355. [[CrossRef](#)]
34. Tabata, N.; Sato, H. Development of the Privacy Consciousness Scale (PCS). *Jpn. J. Personal.* **2014**, *23*, 49–52.
35. Trepte, S.; Teutsch, D.; Masur, P.K.; Eicher, C.; Fischer, M.; Hennh ofer, A.; Lind, F. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European Data Protection Law*; Gutwirth, S., Leenes, R., de Hert, P., Eds.; Springer: Dordrecht, The Netherlands, 2015; pp. 333–365. [[CrossRef](#)]
36. Darmaningrat, E.W.T.; Astuti, H.M.; Alfi, F. Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students. *J. Inf. Syst. Eng. Bus. Intell.* **2020**, *6*, 159–168. [[CrossRef](#)]
37. Zhu, R.; Srivastava, A.; Sutanto, J. Privacy-deprived e-commerce: The efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. *Inf. Technol. People* **2020**, *33*, 1601–1626. [[CrossRef](#)]
38. Mutambik, I.; Lee, J.; Almuqrin, A.; Zhang, J.Z.; Homadi, A. The Growth of Social Commerce: How It Is Affected by Users' Privacy Concerns. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 725–743. [[CrossRef](#)]
39. Mutambik, I.; Lee, J.; Almuqrin, A.; Zhang, J.Z.; Baihan, M.; Alkhanifer, A. Privacy Concerns in Social Commerce: The Impact of Gender. *Sustainability* **2023**, *15*, 12771. [[CrossRef](#)]
40. Mulia, R.A.; Azzahro, F.; Handayani, P.W. Analysis of Internal and External Factors Affecting Online Privacy Concern in E-commerce: Comparative Study by Gender. In Proceedings of the 2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Depok, Indonesia, 17–18 October 2020; pp. 187–192. [[CrossRef](#)]
41. Andrews, V.D. In-Depth Analysis of College Students' Data Privacy Awareness. Master's Thesis, TSYS School of Computer Science, Columbus, GA, USA, 2020.
42. Mekovec, R.; Vrček, N. Factors that influence Internet users' privacy perception. In Proceedings of the ITI 2011—33rd International Conference on Information Technology Interfaces, Cavtat, Croatia, 27–30 June 2011; pp. 227–232.
43. 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. [[CrossRef](#)]
44. Takavarasha, S. Jr.; Chinyamurindi, W.; Chinyamurindi, W. The African Digital Citizen's Awareness of Online Information Privacy. In Proceedings of the 5th Annual ACIST, Addis Ababa, Ethiopia, 2 August 2019.
45. Mtjwara, A.G.; Abdullah, H. Evaluation of the effectiveness of information privacy protection awareness for e-commerce consumers. In Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; IEEE: New York, NY, USA, 2022; pp. 1–8.
46. Chawla, N.; Kumar, B. E-Commerce and Consumer Protection in India: The Emerging Trend. *J. Bus. Ethics* **2022**, *180*, 581–604. [[CrossRef](#)]
47. Markos, E.; Milne, G.R.; Peltier, J.W. Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *J. Public Policy Mark.* **2017**, *36*, 79–96. [[CrossRef](#)]
48. D'Adamo, I.; González-Sánchez, R.; Medina-Salgado, M.S.; Settembre-Blundo, D. E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability* **2021**, *13*, 6752. [[CrossRef](#)]
49. Anic, I.D.; Škare, V.; Kursan Milaković, I. The determinants and effects of online privacy concerns in the context of e-commerce. *Electron. Commer. Res. Appl.* **2019**, *36*, 100868. [[CrossRef](#)]
50. Adelola, T. Developing a Framework for E-Commerce Privacy and Data Protection in Developing Nations: A Case Study of Nigeria. Ph.D. Thesis, Loughborough University, Loughborough, UK, 2017.
51. Al-Jabri, I.; Eid, M.; Abed, A. The willingness to disclose personal information: Trade-off between privacy concerns and benefits. *Inf. Comput. Secur.* **2020**, *28*, 161–181. [[CrossRef](#)]
52. Bandara, R.; Fernando, M.; Akter, S. Privacy concerns in E-commerce: A taxonomy and a future research agenda. *Electron. Mark.* **2020**, *30*, 629–647. [[CrossRef](#)]
53. Smith, H.J.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989–1015. [[CrossRef](#)]
54. Hollebeek, L.D.; Kumar, V.; Srivastava, R.K.; Lim, W.M.; Urbanavicius, S. Guidelines for Theory Selection: The IMPACT Framework. *Psychol. Mark.* **2025**, *42*, 2789–2806. [[CrossRef](#)]
55. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Processes* **1991**, *50*, 179–211. [[CrossRef](#)]
56. Laufer, R.S.; Wolfe, M. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *J. Soc. Issues* **1977**, *33*, 22–42. [[CrossRef](#)]
57. Tang, J.; Akram, U.; Shi, W. Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *J. Enterp. Inf. Manag.* **2020**, *34*, 1097–1120. [[CrossRef](#)]
58. Liu, R. The Influence of Privacy Awareness and Privacy Self-Efficacy in E-Commerce. Master's Thesis, The University of North Carolina at Greensboro (UNCG), Greensboro, NC, USA, 2015.

59. Budak, J.; Rajh, E.; Slijepčević, S.; Škrinjarić, B. Conceptual Research Framework of Consumer Resilience to Privacy Violation Online. *Sustainability* **2021**, *13*, 1238. [\[CrossRef\]](#)
60. Ibdah, D.; Lachtar, N.; Raparathi, S.M.; Bacha, A. “Why Should I Read the Privacy Policy, I Just Need the Service”: A Study on Attitudes and Perceptions Toward Privacy Policies. *IEEE Access* **2021**, *9*, 166465–166487. [\[CrossRef\]](#)
61. Buck, C.; Dinev, T.; Anaraky, R.G. Revisiting APCO. In *Modern Socio-Technical Perspectives on Privacy*; Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 43–60. [\[CrossRef\]](#)
62. Sun, T. Effects of Social Network Sites on Social Capital and Awareness of Privacy: A Study of Chinese and U.S. College Students’ Usage of Social Network Sites. Master’s Thesis, Ohio University, Edinburg, UK, 2014.
63. Ebert, N.; Alexander Ackermann, K.; Scheppeler, B.o. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In *CHI ’21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021*; Association for Computing Machinery: New York, NY, USA, 2021. [\[CrossRef\]](#)
64. Conner, M. Health Behaviors. In *International Encyclopedia of the Social & Behavioral Sciences*; Smelser, N.J., Baltes, P.B., Eds.; Pergamon: Oxford, UK, 2001; pp. 6506–6512. [\[CrossRef\]](#)
65. Alshehri, A.; Clarke, N.; Li, F. A Holistic Framework for Enhancing Privacy Awareness. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6. [\[CrossRef\]](#)
66. Friedewald, M.; Pohoryles, R.J. Technology and privacy. *Innov. Eur. J. Soc. Sci. Res.* **2013**, *26*, 1–6. [\[CrossRef\]](#)
67. Eri, Z.D.; Yusoff, S.; Ngo, K.L.; Ishak, S.N.H.; Ahmad, N. Privacy awareness on cloud storage among students at tertiary level: A case study. *J. Phys. Conf. Ser.* **2020**, *1529*, 022043. [\[CrossRef\]](#)
68. Alashwali, E.; Cranor, L. Privacy Perceptions and Behaviors of Google Personal Account Holders in Saudi Arabia. In Proceedings of the HCI for Cybersecurity, Privacy and Trust, Washington, DC, USA, 29 June–4 July 2024; Springer: Cham, Switzerland, 2024; pp. 3–29.
69. Norman, P.; Conner, M. Health Behavior. In *Reference Module in Neuroscience and Biobehavioral Psychology*; Elsevier: Amsterdam, The Netherlands, 2017. [\[CrossRef\]](#)
70. Chaudhuri, R.; Chatterjee, S.; Vrontis, D. Antecedents of privacy concerns and online information disclosure: Moderating role of government regulation. *EuroMed J. Bus.* **2022**, *18*, 467–486. [\[CrossRef\]](#)
71. Shen, X.; Alashwali, E.; Cranor, L. What Do Privacy Advertisements Communicate to Consumers? *Proc. Priv. Enhancing Technol.* **2024**, *2024*, 466–502. [\[CrossRef\]](#)
72. Xu, H.; Dinev, T.; Smith, H.J.; Hart, P.J. Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View. In Proceedings of the International Conference on Interaction Sciences, Seoul, Republic of Korea, 10–12 January 2008.
73. Bélanger, F.; Crossler, R.E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Q.* **2011**, *35*, 1017–1041. [\[CrossRef\]](#)
74. Ahmad, H.; Halim, H. Determining Sample Size for Research Activities: The Case of Organizational Research. *Selangor Bus. Rev.* **2017**, *2*, 20–34.
75. Hair, J.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publishing: Thousand Oaks, CA, USA, 2022.
76. Urban, T.; Tatang, D.; Degeling, M.; Holz, T.; Pohlmann, N. Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In *ASIA CCS ’20, Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, 5–9 October 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 222–235. [\[CrossRef\]](#)
77. Shehu, V.P.; Shehu, V. Human rights in the technology era—Protection of data rights. *Eur. J. Econ. Law Soc. Sci.* **2023**, *7*, 1–10. [\[CrossRef\]](#)
78. Al Hamli, S.S.; Sobaih, A.E.E. Factors Influencing Consumer Behavior towards Online Shopping in Saudi Arabia Amid COVID-19: Implications for E-Businesses Post Pandemic. *J. Risk Financ. Manag.* **2023**, *16*, 36. [\[CrossRef\]](#)
79. Alshomrani, N.; Furnell, S.; He, Y. Assessing User Understanding, Perception and Behaviour with Privacy and Permission Settings. In *Proceedings of the HCI for Cybersecurity, Privacy and Trust*; Moallem, A., Ed.; Springer: Cham, Switzerland, 2023; pp. 557–575.
80. Stern, T.; Kumar, N. Improving privacy settings control in online social networks with a wheel interface. *J. Assoc. Inf. Sci. Technol.* **2014**, *65*, 524–538. [\[CrossRef\]](#)
81. von Zezschwitz, E.; Chen, S.; Stark, E. “It builds trust with the customers”—Exploring User Perceptions of the Padlock Icon in Browser UI. In Proceedings of the 2022 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 22–26 May 2022; pp. 44–50. [\[CrossRef\]](#)
82. Yuniar, A.D. Thin privacy boundaries: Proximity and accessibility of E-commerce privacy policy in young consumers of Indonesia. *Int. J. Soc. Econ.* **2024**, *51*, 1182–1194. [\[CrossRef\]](#)

83. Urbonavičius, S.; Degutis, M.; Zimaitis, I.; Škare, V. Impacts of store trust antecedents on willingness to disclose personal data in online shopping. *Organ. Mark. Emerg. Econ.* **2023**, *14*, 242–259. [[CrossRef](#)]
84. Alamir, I. Extended Technology Acceptance Model (TAM) for Evaluating Digital Banking Adoption in Saudi Arabia. *Sci. J. King Faisal Univ. Humanit. Manag. Sci.* **2024**, *26*, 63–70. [[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.