

**EXPLORING THE FACTORS AFFECTING ONLINE TRUST IN B2C E-COMMERCE  
TRANSACTIONS IN INDIA: AN EMPIRICAL STUDY**

**Mohammed Alhashem<sup>A</sup>, Mohammed Kamalun Nabi<sup>B</sup>, Ravinder Pant<sup>C</sup>, Asra Inkesar<sup>D</sup>, Nusrat Khan<sup>E</sup>, Mohammed Arshad Khan<sup>F</sup>**



ARTICLE INFO	ABSTRACT
<p><b>Article history:</b></p> <p><b>Received</b> 01 September 2023</p> <p><b>Accepted</b> 14 December 2023</p>	<p><b>Purpose:</b> The COVID-19 pandemic has led to a surge in e-commerce as millions of people were forced to stay at home and adopt digital channels for their purchases to avoid crowded supermarkets. It made the whole world look towards e-commerce as a one-stop solution for keeping markets alive. However, it came as an opportunity for digital fraudsters as a huge number of digital frauds were reported during this pandemic. Such incidents raised questions about online trust-related issues. Fake websites, insecure payment mechanisms, data theft, privacy breach, product reliability, etc., are a few of the reasons why many people are still not confident about using e-commerce platforms. When customers cannot physically touch, feel, and see the products, it becomes even more suspicious and raises serious uncertainty about the quality of the promised product and transaction setup in the e-commerce framework.</p> <p><b>Design/Methodology/Approach:</b> In this study, primary data was collected through structured questionnaires from e-commerce website users belonging to Generation Z and analyzed using Structural Equation Modelling and Path Analysis in IBM SPSS AMOS version 24.</p>
<p><b>Keywords:</b></p> <p>Online Trust; Online Security and Privacy; Website Appearance; Purchase Intention; Generation Z; COVID-19.</p>	<p><b>Findings:</b> Online Security, Online Privacy, and Website appearance were studied and found to have a significant positive impact on online trust. Online trust was also found to be a predictor of purchase intention. Online trust was also found to act as a full mediator between online security and purchase intention, online privacy, and purchase intention, and as a partial mediator between website appearance and purchase intention.</p> <p><b>Research, Practical &amp; Social Implications:</b> The cross-sectional nature of this study makes it difficult for making inferences about causal relationships so new studies can adopt and check the utility of a longitudinal approach in this area. Furthermore, the data collected using convenience sampling had all young generation respondents, mostly college/university students. This current study takes only three antecedents of online trust with reference to a young generation; an exploratory study is needed here to find out new possible antecedents of developing online trust. Moreover, the appearance of the website is altogether a vast area to investigate for further development; very limited dimensions of the appearance of e-commerce websites are covered in this study.</p> <p>Doi: <a href="https://doi.org/10.26668/businessreview/2023.v8i12.3945">https://doi.org/10.26668/businessreview/2023.v8i12.3945</a></p>



<sup>A</sup> Ph.D in Management. College of Administration and Financial Science, Saudi Electronic University Riyadh 11673. Saudi Arabia. E-mail: [m.alhashem@seu.edu.sa](mailto:m.alhashem@seu.edu.sa) Orcid: <https://orcid.org/0000-0002-9244-8413>

<sup>B</sup> Ph.D in Commerce. Department of Commerce and Business Studies, Jamia Millia Islamia a Central University. New Delhi, India. E-mail: [mnabi@jmi.ac.in](mailto:mnabi@jmi.ac.in) Orcid: <https://orcid.org/0000-0002-9230-4225>

<sup>C</sup> Master in Commerce. Department of Commerce and Business Studies, Jamia Millia Islamia a Central University. New Delhi, India. E-mail: [rpantscholar@gmail.com](mailto:rpantscholar@gmail.com) Orcid: <https://orcid.org/0000-0002-7298-0859>

<sup>D</sup> Ph.D in Commerce. College of Administration and Financial Science, Saudi Electronic University Riyadh 11673. Saudi Arabia. E-mail: [a.inkesar@seu.edu.sa](mailto:a.inkesar@seu.edu.sa) Orcid: <https://orcid.org/0000-0003-1957-1084>

<sup>E</sup> Ph.D in Commerce. College of Administration and Financial Science, Saudi Electronic University Riyadh 11673. Saudi Arabia. E-mail: [n.khan@seu.edu.sa](mailto:n.khan@seu.edu.sa) Orcid: <https://orcid.org/0000-0002-7549-0329>

<sup>F</sup> PhD in Commerce and Business Studies. College of Administration and Financial Science, Saudi Electronic University Riyadh 11673. Saudi Arabia. E-mail: [m.akhan@seu.edu.sa](mailto:m.akhan@seu.edu.sa)

## EXPLORANDO OS FATORES QUE AFETAM A CONFIANÇA ONLINE NAS TRANSAÇÕES DE COMÉRCIO ELETRÔNICO B2C NA ÍNDIA: UM ESTUDO EMPÍRICO

### RESUMO

**Objetivo:** a pandemia da Covid-19 levou a um aumento do comércio eletrônico, à medida que milhões de pessoas foram forçadas a ficar em casa e adotar canais digitais para suas compras a fim de evitar supermercados lotados. Fez com que o mundo inteiro olhasse para o comércio eletrônico como uma solução única para manter os mercados vivos. No entanto, essa foi uma oportunidade para os fraudadores digitais, já que um grande número de fraudes digitais foram relatadas durante essa pandemia. Tais incidentes levantaram questões sobre questões relacionadas com a confiança em linha. Sites falsos, mecanismos de pagamento inseguros, roubo de dados, violação de privacidade, confiabilidade do produto, etc., são algumas das razões pelas quais muitas pessoas ainda não estão confiantes sobre o uso de plataformas de comércio eletrônico. Quando os consumidores não conseguem tocar, sentir e ver fisicamente os produtos, torna-se ainda mais suspense e levanta sérias incertezas sobre a qualidade do produto prometido e configuração da transação no quadro do comércio eletrônico.

**Design/Methodologia/Abordagem:** Neste estudo, os dados primários foram coletados por meio de questionários estruturados de usuários de sites de comércio eletrônico pertencentes à Geração Z e analisados utilizando Modelagem de Equação Estrutural e Análise de Caminho no IBM SPSS AMOS versão 24.

**Constatações:** Segurança Online, Privacidade Online e Aparência do Site foram estudadas e consideradas como tendo um impacto positivo significativo na confiança online. A confiança online também foi considerada um preditor de intenção de compra. Também se descobriu que a confiança online atua como um mediador completo entre a segurança online e a intenção de compra, a privacidade online e a intenção de compra, e como um mediador parcial entre a aparência do site e a intenção de compra.

**Investigação, Implicações Práticas e Sociais:** A natureza transversal deste estudo dificulta a realização de inferências sobre as relações causais para que novos estudos possam adotar e verificar a utilidade de uma abordagem longitudinal nesta área. Além disso, os dados coletados por meio de amostragem de conveniência tinham todos os jovens entrevistados da geração, principalmente estudantes universitários. O presente estudo tem apenas três antecedentes de confiança online em relação a uma geração jovem; um estudo exploratório é necessário aqui para descobrir novos possíveis antecedentes do desenvolvimento da confiança online. Além disso, o aparecimento do site é uma vasta área a ser investigada para desenvolvimento adicional; dimensões muito limitadas do aparecimento de sites de comércio eletrônico são abordadas neste estudo.

**Palavras-chave:** Confiança Online, Segurança e Privacidade Online, Aparência de Site, Intenção de Compra, Geração Z, Covid-19.

## EXPLORANDO LOS FACTORES QUE AFECTAN LA CONFIANZA EN LÍNEA EN LAS TRANSACCIONES DE COMERCIO ELECTRÓNICO B2C EN INDIA: UN ESTUDIO EMPÍRICO

### RESUMEN

**Propósito:** La pandemia de COVID-19 ha provocado un aumento del comercio electrónico, ya que millones de personas se vieron obligadas a quedarse en casa y adoptar canales digitales para sus compras para evitar supermercados atestados. Hizo que todo el mundo mirara hacia el comercio electrónico como una solución integral para mantener vivos los mercados. Sin embargo, llegó como una oportunidad para los estafadores digitales, ya que un gran número de fraudes digitales fueron reportados durante esta pandemia. Tales incidencias plantearon preguntas sobre cuestiones relacionadas con la confianza en línea. Sitios web falsos, mecanismos de pago inseguros, robo de datos, violación de la privacidad, confiabilidad del producto, etc., son algunas de las razones por las que muchas personas todavía no confían en el uso de plataformas de comercio electrónico. Cuando los clientes no pueden tocar físicamente, sentir y ver los productos, se vuelve aún más suspi y genera una seria incertidumbre sobre la calidad del producto prometido y la configuración de la transacción en el marco del comercio electrónico.

**Diseño/Methodología/Enfoque:** En este estudio, los datos primarios se recopilaron a través de cuestionarios estructurados de usuarios de sitios web de comercio electrónico pertenecientes a la Generación Z y se analizaron utilizando el Modelado de Ecuaciones Estructurales y el Análisis de Rutas en IBM SPSS AMOS versión 24.

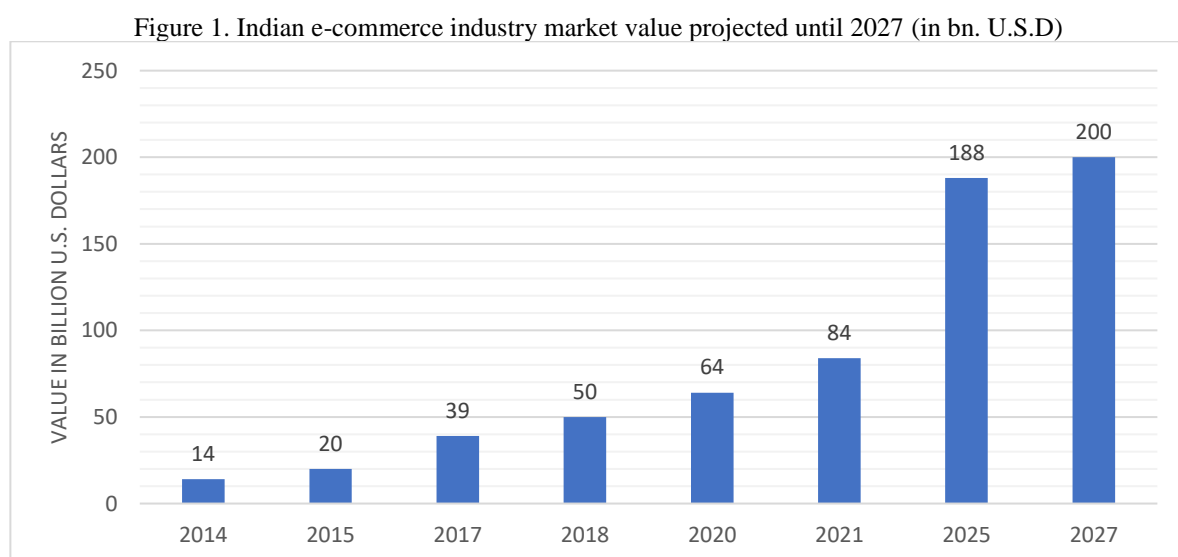
**Hallazgos:** Se estudió la seguridad en línea, la privacidad en línea y la apariencia del sitio web y se encontró que tienen un impacto positivo significativo en la confianza en línea. La confianza en línea también resultó ser un preditor de la intención de compra. También se encontró que la confianza en línea actúa como un mediador completo entre la seguridad en línea y la intención de compra, la privacidad en línea y la intención de compra, y como un mediador parcial entre la apariencia del sitio web y la intención de compra.

**Implicaciones Investigativas, Prácticas y Sociales:** El carácter transversal de este estudio dificulta hacer inferencias sobre las relaciones causales, por lo que nuevos estudios pueden adoptar y comprobar la utilidad de un enfoque longitudinal en esta área. Además, los datos recogidos mediante muestreo por conveniencia incluyeron a todas las generaciones de jóvenes encuestados, en su mayoría estudiantes universitarios. El presente estudio toma solo tres antecedentes de la confianza en línea con referencia a una generación joven; aquí se necesita un estudio exploratorio para encontrar nuevos posibles antecedentes de desarrollo de la confianza en línea. Por otra parte, la aparición del sitio web es en conjunto un amplio ámbito de investigación para su posterior desarrollo; en este estudio se abordan dimensiones muy limitadas de la aparición de sitios web de comercio electrónico.

**Palabras clave:** Confianza en Línea, Seguridad y Privacidad en Línea, Apariencia en el Sitio Web, Intención de Compra, Generación Z, COVID-19.

## INTRODUCTION

A rapidly increasing global digital population and internet userbase has empowered e-commerce to become a crucial part of the worldwide retail system. The growing importance of e-commerce can be inferred from the fact that approximately 1.92 billion consumers purchased goods and services over the internet in 2019 and e-retail sales crossed 3.5 trillion USD globally in the same year (Daniela Coppola, 2021). A massive number of 560 million internet users make India stand as the second largest digital market in the world. This is just half the picture, as the internet penetration rate stood at around 50 percent in 2020 which makes it a big potential digital market. An estimate says that there will be more than 650 million internet users in 2023 (Sandhya Keelery, 2020). At this rate of growth among digital users and internet adopters, the forecasted market valuation of the Indian e-commerce industry by 2027 will touch the mark of 200 billion USD (BCG; Bain and Company; Morgan Stanley, 2020).



Source: (BCG; Bain and Company; Morgan Stanley, 2020).

The e-commerce industry of India offers fierce competition as currently it is occupied by local as well as multinational companies. The COVID-19 pandemic has also caused a significant impact on business and consumer behaviors. It has redefined the patterns of consumption and the habits of consumers, altering purchase behavior and posing a challenge for businesses to overcome. This involves getting back on the track of sustainable growth after the pandemic as well as making customers loyal to e-commerce shops (Donthu and Gustafsson, 2020). Previous literature gives the argument that trust is one of the vital factors which influence a customer's online behavioral intentions in the form of intentions to make repeat purchases (Hong and Cho, 2011; M. S. Kim and Ahn, 2007; Pavlou and Gefen, 2004). Continuous advancement in technology and the epidemic caused by coronavirus have pushed the further digitalization, mass adoption, and development of e-commerce (Santo and Marques, 2022). Variations in consumption patterns and behaviors along with the policies of governments under the pandemic situation have affected the environment of the cyberworld. Where users were busy enjoying the benefits of e-commerce and online shopping, not all participants and vendors were authentic (Ma and McKinnon, 2022). This pandemic has paved the way for new patterns of digital frauds that were either not heard of in the past or were not widespread in the past (Boman and Gallupe, 2020). Many businesses are now securing their transactions as unconventional methods of frauds are used increasingly on a bigger scale and more frequently. Ultimately the risk profile of e-commerce and fintech institutions has increased significantly during this pandemic (Karpoff, 2020). The pandemic has caused many emotional and psychological sufferings for people such as stress, depression, anxiety, loneliness, insomnia, and suicidality (Lee, 2020). The most vulnerable target for cybercriminals are people who are suffering psychologically, as it is easy to manipulate the emotional instabilities of the anxious user to take advantage of them and commit cyber fraud (Ma and McKinnon, 2022). Security-related issues with e-commerce can also be taken as a threat which needs to be eliminated for the sustainable development of digital commerce (Pabian, Pabian, and Reformat, 2020). Sometimes, these fraudsters use emotional appeal to encourage victims to buy services (Naidoo, 2020). All such events make it difficult for e-commerce businesses to establish trust during such pandemic times. However, online fraud and cybercrime is not brand new; it even existed before the pandemic when people were not educated and informed about the e-commerce world (Karpoff, 2020). However, the pandemic has increased online transactions and e-commerce exponentially, which has amplified the problem because the opportunities available for such crimes have increased (Wronka, 2022). Furthermore, it is comparatively difficult to detect and

prevent due to the high volume and the frequencies of daily transactions (Lallie et al., 2021). Developing an e-commerce platform is way more complex than it seems. It is not like you establish it once and then stay idle for its lifetime. Many times, it is reported by users that prices of similar products are listed differently, a discount coupon is not applied properly, an out-of-stock item is still online, a link is not working, a shipping cost is incorrectly applied, etc. Customers may get furious over such issues and feel frustrated with your e-commerce website's uncooperating design. An e-commerce website is required to engage with users, feeding information and awareness about the product, nurturing them from visitors to buyers, providing them with reviews and ratings, and many more management-related tasks. The role of the website is changing continuously and becoming a sort of tool which can create customer profiles, save addresses and likings, use search history to suggest better items, accept reviews and ratings, communicate with users via SMS or email, process orders, manage pickup updates, ship orders, and make reports, all at the same time. Managing all these tasks along with ensuring security and privacy and developing trust is really a complex subjective process. Potential buyers feel uncomfortable while making online transactions through seller's websites, believing that shopping through online channels is riskier than the old traditional method of shopping (Y. Kim and Peterson, 2017). Especially in India, people are still unwilling to trust digital payments for e-commerce platforms, but providing a strong cybersecurity framework and infrastructure will eventually make them adopt e-commerce along with its digital payment mechanisms (Khan, 2021). That is why e-commerce companies are now focusing on increasing their profitability by making their e-commerce systems and online purchasing processes easier and safer from the perspective of a buyer (D. J. Kim et al. 2016; Quach and Thaichon, 2017).

The objective of this study is to determine the impact of online security, online privacy, and website appearance on building online trust towards B2C e-commerce in India and its impact on the intentions of Generation Z users to make purchases. Against such a backdrop, we endeavored to contribute to, and broaden the scope of, the literature by developing a theoretical model of factors affecting online trust, where they influence online trust towards e-commerce websites, which in turn leads to the development of purchase intentions in the context of e-commerce.

## **THEORETICAL REFERENTIAL**

Looking at such a huge e-commerce market, numerous sellers enter the industry to try their luck and entrepreneurial potential. This makes the industry highly competitive, more

uncertain, and even more difficult for customers to develop online trust towards sellers (Martin et al., 2015). Dibb (2010) and Chen et al. (2014) gave arguments in support of the argument that trust towards an e-commerce website is significantly associated with attitudes towards the website and the same has been supported by several empirical studies (Pennington et al. 2003). Various existing examples in the literature were reviewed to get deeper into the above subject and a list of factors affecting trust towards an e-commerce website was generated. Out of these factors we have chosen the three most common factors: online security, online privacy, and website appearance.

### **Online Security and Privacy**

Security and privacy collectively refer to the scenarios where e-commerce websites are adopting effective methods to protect the personal and private data of their users from getting misused by hackers and digital thieves (D. J. Kim et al., 2008). It means all the steps taken by the website to ensure a safe environment and to protect consumers from any leakage of information (Forsythe and Shi, 2003; D. J. Kim et al., 2008; Vinerean et al., 2013; Weisberg et al., 2011). People always fear the hijacking and misutilization of personal information and that is why reluctant behavior is demonstrated by them while submitting any personal information on e-commerce websites. People hesitate to submit any personal information and feel even more fearful while giving financial particulars on a website (Lim, 2003). The moment a customer perceives a sense of security and privacy, their level of trust seems to increase accordingly. In cases where either the e-commerce website is little known or the user is unfamiliar with it, there are chances of higher risk, and this negatively affects the intention to purchase. A good sense of security can be developed among users through ensuring that a major contribution of information technology concerns establishing sufficient security features and privacy protection mechanisms (Pavlou et al., 2007). Relatedly, a consumer who trusts an e-commerce website also has a significant effect on the risk associated with the disclosure of information on the site. (Zimmer et al., 2010). In such a payment and transaction setup, where due consideration is being given to security and privacy, consumers automatically trust the websites for making exchanges in the online mode (Forsythe and Shi, 2003; D. J. Kim et al., 2008; Weisberg et al., 2011). Applications of advanced technology in security mechanisms aimed to protect consumers from fraud, hacking or phishing, positively impact online trust towards the e-commerce platform and a consumer's purchase intentions. Online security can be defined as the "application of advanced techniques that can help prevent the users from risk

of fraud, hacking or phishing” (D. J. Kim et al., 2008; Lian and Lin, 2008; Roca et al., 2009; Yousafzai et al., 2003). Such techniques should be capable of preventing all the attempts of illegal data access, misuse of data, and ensuring the safety of data (Ponirir et al., 2015; Shalhoub, 2006). Security is categorized as one critical factor of online trust (Salimon et al., 2015). Flavián and Guinalú (2006) concluded in their study that trust can be enhanced especially by developing a sense of security in consumers who use the systems adopted by the e-commerce website. The attitude of the consumers towards e-commerce businesses is explained using the confidence of trust, privacy, and safety of any information or data given by the consumer (Abri et al., 2009; Salam et al., 2005). Customers consider privacy and security as a spontaneous feature and therefore develop increased confidence in online transactions (Al-Adwan and Al-Horani, 2019). Therefore, if security and privacy systems are set and policies clearly disclosed, the trust of the users can be won which in turn facilitates transactions over the online network (Chellappa and Pavlou, 2002). The following hypotheses are proposed based on the above literature review:

**H<sub>1</sub>.** Online Security positively affects consumer’s online trust.

**H<sub>2</sub>.** Online Privacy positively affects consumer’s online trust.

### **Website Appearance**

Website appearance is the first impression of the e-commerce portal which gives a basic idea about the seller, their products, their area of operations, and their style of working. It is the visual impression and appeal of any website (Dibb, 2010). The appearance of a website is considered as an important gateway towards the development of perceived quality of that website (S. Kim and Stoel, 2004b, 2004a). Whatever an e-commerce company is offering to the market can only be seen and accessed through its website, so it is the only point of interaction between the company and the customers. Website appearance is the reflection of a company’s perception of design, security, and privacy policies and the ease and convenience of its business; it is the self-presentation of the e-commerce website. E-commerce websites do not have any human or social touch and the vendor is invisible, so website appearance emerges as an online storefront which formulates the first impression of the website (Harrison et al., 2002; Shen and Khalifa, 2012; Szymanski and Hise, 2000). The appearance of a website helps in convincing consumers about the trustworthiness of the platform. One should evaluate the performance of any e-commerce website on how it offers cues to consumers for developing conviction towards the trustworthiness of the website (Gefen et al., 2004). A website’s

appearance and design and content placement help to boost the sense of trust (Cyr et al., 2010; Harrison M. et al., 2002). Customers are unwilling to perform transactions through a website which is unable to provide a sense of trust (Al-Adwan and Al-Horani, 2019). Trustworthiness of the payment gateways and transaction partners when reflected by websites can eventually be a deciding parameter of trust. According to the previously mentioned studies, our next hypothesis is:

**H3.** Appearance of e-commerce websites positively affects consumers' online trust.

### Online Trust and Purchase Intention

Online trust is a vital element for the development of satisfaction among customers and securing the expected results in the purchase intentions through online transactions (Flavián and Guinalú, 2006; David Gefen and Straub, 2004; Pavlou and Gefen, 2004; Wu and Chen, 2005; Yousafzai et al., 2003). Various Scholars have segmented the concept of online trust in many ways (Table 1).

Table 1. Different types of online trust

<b>Different Types of Online Trust Studied by Previous Researchers</b>
<i>Trust on the Website</i> (Hsiao et al., 2010; Pavlou and Gefen, 2004; Shu and Chuang, 2011)
<i>Trust on the Vendor</i> (Brotheridge and Zygadlo, 2006; M. S. Kim and Ahn, 2007; Lu et al., 2010; Pavlou and Gefen, 2004)
<i>Trust in the auction's initiator</i> (Kauffman, Lai, and Lin, 2010; Tsvetovat and Sycara, 2000)
<i>Trust in the group members</i> (Lu et al., 2010; Mael and Ashforth, 1992; Shu and Chuang, 2011)

Source: Compiled by the Researchers.

In this study the focus will be especially on trust towards the websites of e-commerce players. Presence of trust signifies that the e-seller is not having any intentions to cheat and take unjustified gains from the customer (Gefen et al., 2003; Sin et al., 2012). Mayer et al. (1995) regarded trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”. When consumers or users develop an intention to transact with a website, this leads to the purchase of product. Willingness to be involved in these online transactions is the situation which is called a purchase intention (Pavlou, 2003). Consumers assess an e-commerce website from the angle of trust and this assessment influences their attitude towards making online transactions on the website, and also their attitude affects their intention to purchase (Wang et al., 2003). Customers' trust in e-retailers can reduce the susceptibility and social complexity that customers perceive in e-commerce settings (Al-Adwan, Alrousan, Yaseen, Alkufahy, and Alsoud, 2022). High trust



perception can substantially control the uncertainty related to the online world and persuade users to go experience online platforms and e-commerce portals (Al-Adwan and Al-Horani, 2019). Many studies support the argument that the intention to purchase a product online is positively driven by online trust (Gefen et al., 2004; Grabner-Kräuter and Kaluscha, 2003; Pavlou, 2003; (Al-Adwan, Al-Debei, and Dwivedi, 2022)). On the same above lines, our fourth and last proposed hypothesis is:

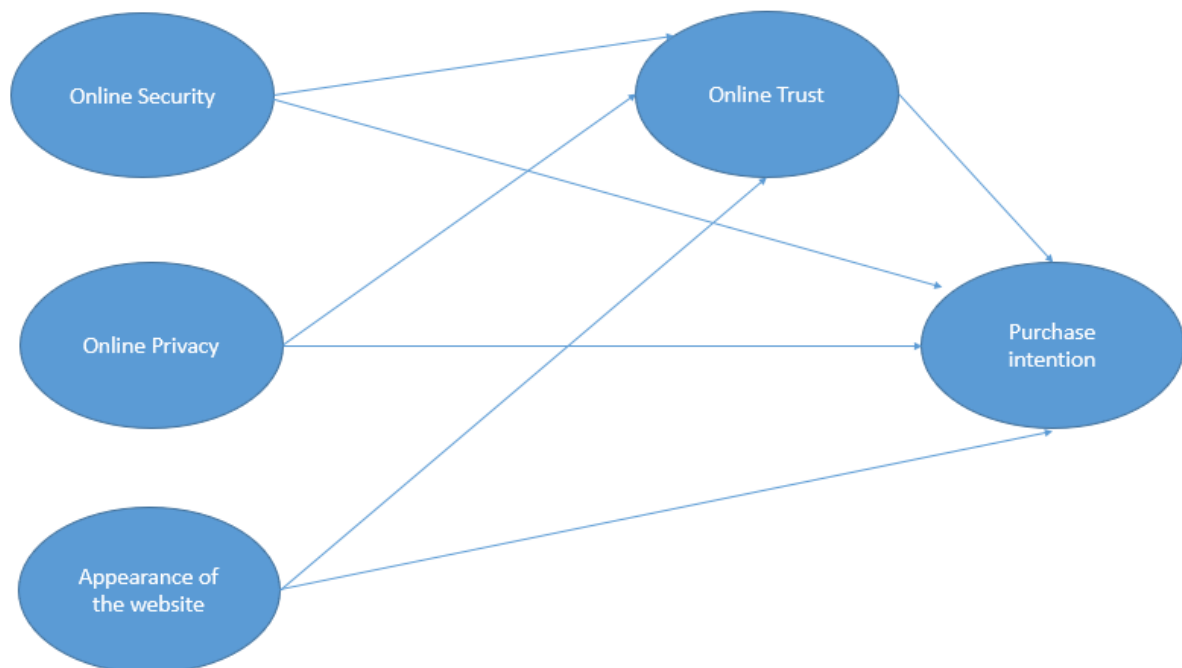
**H4.** Online Trust positively affects the Purchase Intention on e-commerce websites.

**H5.** There is a significant impact of online trust as a mediating variable on the relationship between online security and purchase intention.

**H6.** There is a significant impact of online trust as a mediating variable on the relationship between online privacy and purchase intention.

**H7.** There is a significant impact of online trust as a mediating variable on the relationship between website appearance and purchase intention.

Figure 2. Proposed Conceptual Model



Source: Based on hypotheses developed by the researchers.

## RESEARCH METHODOLOGY

A comprehensive study of online security, privacy, online trust, and purchase intention was conducted to achieve the objectives of this study. Primary data was collected using a structured questionnaire. A descriptive research design involving surveys and literature assistance was selected for this study. This study used a non-experimental approach, which

relies on measurement, and does not involve the intervention of the researchers. Researchers used emails and social media channels to distribute the questionnaire as it was not possible to do otherwise due to the ongoing pandemic. Overall, this study is correlational and cross-sectional in nature.

### **Population and Sample**

The population for this study consisted of Generation Z (born between 1995–2009) users of e-commerce websites (Goh and Lee, 2018). However, given limited accessibility to this population, as well as limited resources and time, a total of 251 samples were collected from a convenience sampling through Google forms. The convenience sampling technique is the easiest one to adopt without any funding and resources availability (Malhotra and Dash, 2016). The sample size in this study is thought to sufficiently represent the relevant population as it was consistent with the 10 times rule whereby a minimum of 190 responses were needed as there were 19 items in the proposed model (Barclay et al. 1995).

### **Survey Instrument Development**

This study adapted validated measures from previous studies where participants scored every item on a five-point Likert scale labelling from *strongly disagree (1) to strongly agree (5)*. Online security (5-items) and online privacy (5-items) were measured using the scale developed by Yousafzai et al. (2003), online trust was measured using a 9-items scale developed by Gefen et al. (2004); Pavlou, (2003); and Shim et al., (2001), website appearance was measured using S. Kim and Stoel's (2004a, 2004b) 6-item scale. To measure purchase intention, a 3-item scale was adapted from the behavioral intention scale of Bhattacharjee (2011) and Mathieson (1991). All the measures of the above constructs have shown acceptable levels of validity in previous studies. However, some statements were modified on wording or language grounds to make them match the context of the current study (i.e., online trust and e-commerce websites) in which the instrument was used. The modified, final questionnaire was shared through a Google form survey.

## **RESULT AND DISCUSSION**

After data collection, the data was imported to IBM SPSS software for data cleaning where missing values were identified and outliers were checked. Finally, a total of 251

responses were collected with all belonging to Generation Z. The detailed demographic profiles are listed in Table 2.

Table 2. Demographic Profile

<b>Gender</b>	<b>N</b>	<b>%</b>
Male	116	46.2
Female	135	53.8
<b>Frequency of accessing E-Commerce Websites</b>		
Daily	23	9.2
2–4 times a week	51	20.3
Once a week	37	14.7
2–4 times a month	62	24.7
Once a month	60	23.9
As and when required	18	7.2
<b>For how long have you been accessing e-commerce websites?</b>		
Less than 6 months	15	6
6–12 months	25	10
1–3 years	129	51.4
3–6 years	61	24.3
6 years or more	21	8.4
<b>Mode of accessing e-commerce websites?</b>		
Through mobile application	149	59.4
Through desktop	4	1.6
Through both	98	39.0

Source: Compiled by the Researchers.

To test the reliability of the construct items, Cronbach’s coefficient alpha was used. All the constructs had Cronbach’s coefficient alpha values ranging from 0.779 to 0.854. As shown in Table 3, all the reliability figures satisfied the conventional recommended cut-off of 0.70 (Hair et al. 2016).

Table 3. Reliability and Convergent validity parameters

<b>Scale</b>	<b>Cronbach’s Alpha</b>	<b>No. of Items</b>	<b>CR</b>	<b>AVE</b>	<b>MSV</b>	<b>ASV</b>
Online Privacy	0.823	4	0.824	0.539	0.500	0.321
Online Security	0.854	4	0.837	0.565	0.521	0.339
Online Trust	0.844	5	0.846	0.521	0.521	0.422
Website Appearance	0.779	3	0.810	0.600	0.350	0.185
Purchase Intention	0.803	3	0.810	0.588	0.483	0.344
Combined Reliability of All Constructs Taken Together	0.913	19				

Source: Compiled by the Researchers. Note: CR = Composite Reliability; AVE = Average Variance Extracted; MSV = Maximum Shared Variance; ASV = Average Squared Shared Variance.

The Kaiser-Meyer-Olkin measure (Table 4) justified the sampling adequacy for the analysis where KMO = 0.887, and all KMO values for individual items range between 0.687 to 0.837, which is above the acceptable limit of 0.50 (Field, 2009).

Table 4. KMO and Bartlett's Test

<b>Kaiser-Meyer-Olkin Measure of Sampling Adequacy.</b>	<b>0.887</b>
	Approx. Chi-Square
	2469.428
<b>Bartlett's Test of Sphericity</b>	Df
	171
	Sig.
	0.000

Source: Compiled by the Researchers.

Table 5 depicts standard deviations, means, and correlation figures. All the proposed study variables were found to have significant correlations with one another ( $p < 0.01$ ). As proposed, online security, online privacy, and web appearance have significant correlations with dependent variables, i.e., online trust ( $r = 0.802^{**}$ ,  $r = 0.745^{**}$ , and  $r = 0.554^{**}$ , respectively, at  $p < 0.01$ ). Additionally, the relationship between online trust and purchase intention is found to be significant ( $r = 0.780^{**}$  at  $p < 0.01$ ).

These initial correlation findings provide support for the study to proceed further and identify causation effects using Structural Equation Modelling.

Table 5. Descriptive Statistics and Correlations

Descriptive Statistics	Correlations						
	Mean	Std. Deviation	N	Website Appearance	Online Privacy	Online Security	Online Trust
<b>Website Appearance</b>	2.4268	0.33997	251	1			
<b>Online Privacy</b>	3.4969	0.58822	251	0.292 **	1		
<b>Online Security</b>	3.3862	0.54115	251	0.319 **	0.799 **	1	
<b>Online Trust</b>	3.4772	0.46459	251	0.554 **	0.745 **	0.802 **	1
<b>Purchase Intention</b>	4.0561	0.54036	251	0.664 **	0.615 **	0.588 **	0.780 **

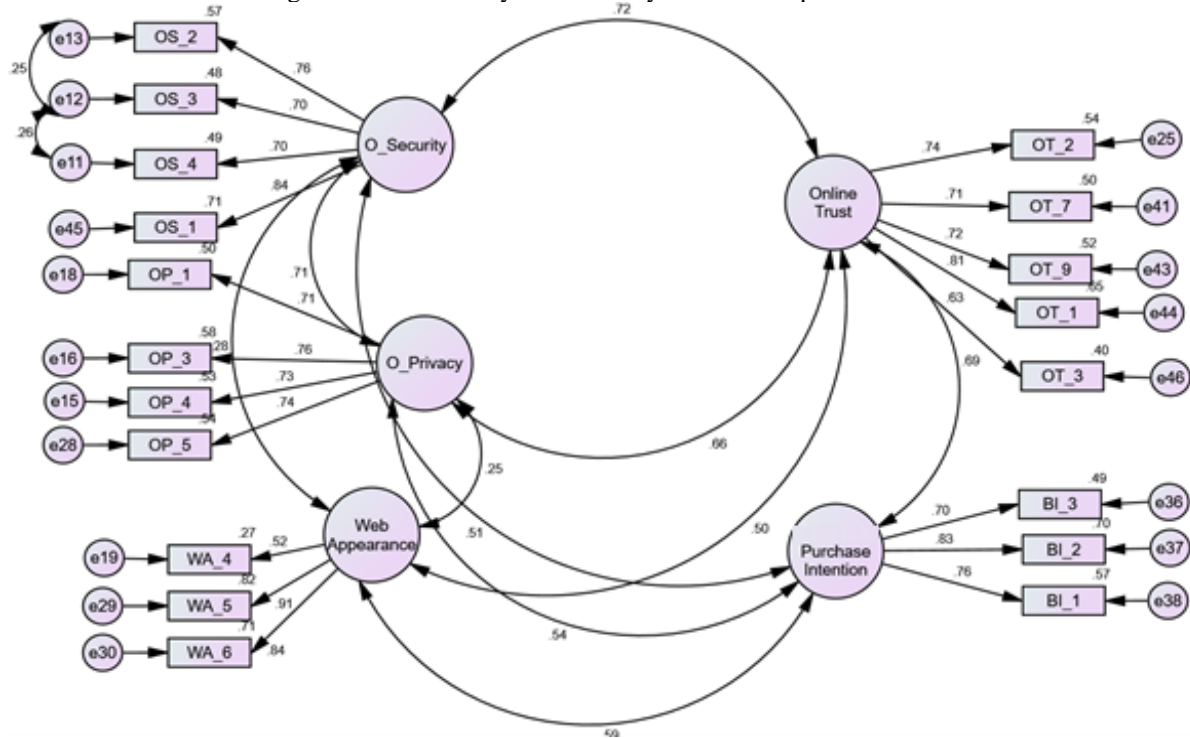
Source: Compiled by the Researchers. \*\* Correlation is significant at the 0.01 level (2-tailed).

## Measurement Model

To test the proposed model researchers used Structural Equation Modeling (SEM). SEM is very useful for testing the direction and strength of the relationships proposed as different hypotheses (Verma, 2021). The overall sample was divided into two sub-groups namely confirmatory and validation. Confirmatory Factor Analysis (CFA) is a multivariate statistical technique which confirms whether or not the measured variables are truly representing the number of constructs. The full measurement model consisted of five constructs and nineteen items (Figure 3).

The initial CFA findings showed a fit according to the predetermined benchmarks when all the latent variables were combined simultaneously in a single model and correlated as a first order factor with Chi-square  $\chi^2 = 309.723$ ,  $df = 140$ ,  $CMIN/df = 2.212$  ( $CMIN/DF < 5$  indicating a reasonable fit; (Wheaton et al., 1977));  $CFI = 0.928$  ( $\geq 0.90$  ; (Bentler, 1990),  $GFI = 0.888$  (Baumgartner and Homburg, 1996), and  $RMSEA = 0.070$  ( $< 0.07$ ; (Steiger, 2007)).

Figure 3. Confirmatory Factor Analysis of the Proposed Model



Source: Extracted using IBM SPSS AMOS 24 by the Researchers.

### Construct Validity

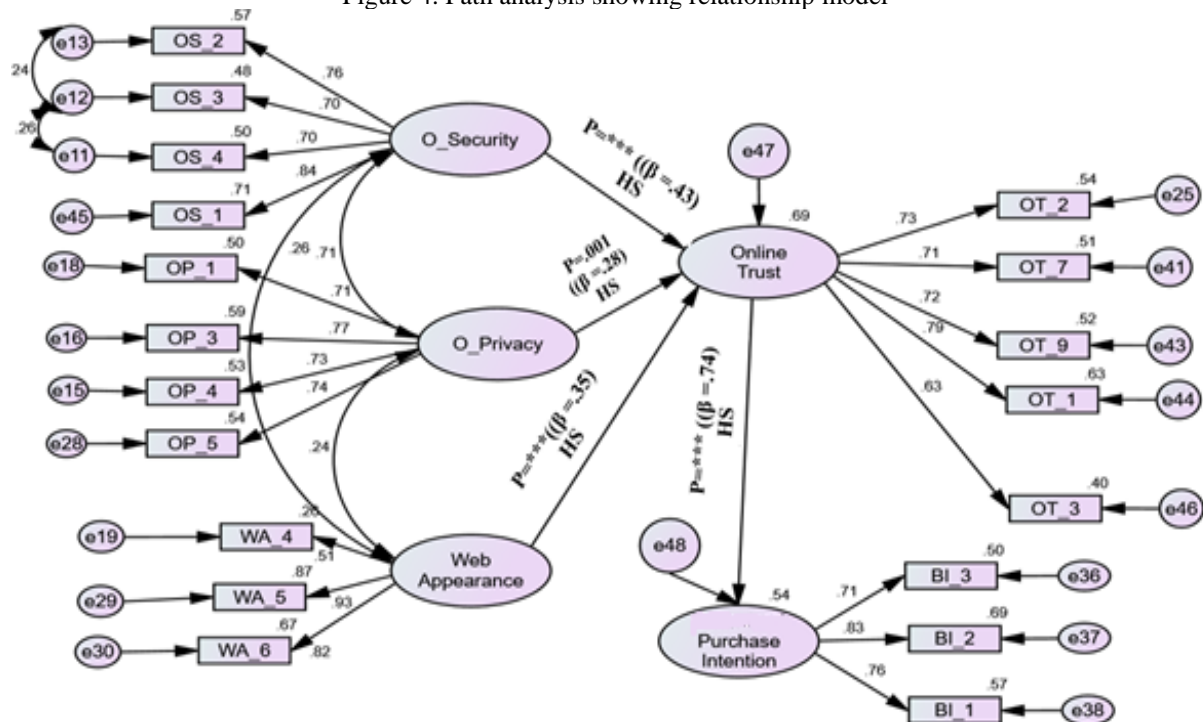
Convergent and discriminant construct validity parameters displayed acceptable values. All items had Standardized Regression Weights (SRW) of greater than 0.70 (Hair et al., 2016). According to Netemeyer et al. (2003), the T value for all loadings was determined to be higher than 2.57, supporting the convergent validity requirements. Furthermore, Average Variance Extracted (AVE) were all greater than 0.50. With  $AVE > MSV$  and  $AVE > ASV$  (Fornell and Larcker, 1981) being used as benchmark parameters, discriminant validity was also supported (Table 3). With the value of Composite Reliability (CR) (Table 3) ranging from 0.810 to 0.846, the recommended level of CR is also achieved ( $CR > 0.70$ , Hair et al., 2016). Moreover, Average Variance Extracted (AVE) for all the constructs was above the threshold limit of 0.50 and  $CR > AVE$  (Hair et al., 2010) (Table 3). With all the parameters satisfying the benchmark criteria of CFA, the next step involves testing hypotheses.

### Relationship Testing and Results

The hypothesized relationships from the proposed model were tested using Structural Equation Modelling (SEM) with the maximum likelihood method in IBM AMOS Version 24. As indicated in Figure 4., the relationship between online security and consumer's online trust is in the hypothesized direction and was found to be statistically significant (Standardized

Beta ( $\beta$ ) = 0.43,  $p < 0.01$ ), thereby supporting the first hypothesis ( $H_1$ ). Similarly, the relationship between online privacy and consumer's online trust ( $H_2$ ) (Standardized Beta ( $\beta$ ) = 0.28,  $p < 0.01$ ), appearance of e-commerce websites and consumers' online trust ( $H_3$ ) (Standardized Beta ( $\beta$ ) = 0.35,  $p < 0.01$ ), and online trust and purchase intention on e-commerce websites ( $H_4$ ) (Standardized Beta ( $\beta$ ) = 0.74,  $p < 0.01$ ) were all in the hypothesized directions and were found to be statistically significant and to have positive impact. Hence, this study supports  $H_2$ ,  $H_3$ , and  $H_4$  as well.

Figure 4. Path analysis showing relationship model



Source: Extracted using IBM SPSS AMOS 24 by the Researchers. Note:  $p = ***$  means  $p < 0.001$ ; HS = Hypothesis Supported.

For testing the hypotheses  $H_5$ ,  $H_6$ , and  $H_7$ , path analysis mediation using AMOS 25 was applied. This study adopted a three-layer regression model as suggested by Baron and Kenny (1986) which states that the independent variable (IDV) is correlated with the mediator Variable (MV) (Path a), the independent variable (IDV) must have an effect over the dependent variable (DV) in the absence of mediating variable (Path b), and the impact of the independent variable (IDV) on the dependent variable (DV) is changed with the addition of the mediating variable in the model (Path c).

To test hypothesis five ( $H_5$ ), all three conditions stated according to Baron and Kenny (1986) are satisfied (Table 6). With Chi-square = 43.954, Degrees of freedom = 24,  $p < 0.001$ ,

CMIN/DF = 1.831, CFI = 0.981, GFI = 0.964, RMR = 0.018 the model satisfies all model fit parameters. Online trust regresses significantly on online security (path a). With Chi-square = 43.003, Degrees of freedom = 11,  $p < 0.001$ , CMIN/DF = 3.909, CFI = 0.958, GFI = 0.955, and RMR = 0.034 the model satisfies all model fit parameters. Purchase intention regresses significantly on online security in absences of mediator. Hence, condition two of Baron and Kenny's Mediating Analysis approach is also satisfied. With Chi-square= 121.409, Degrees of freedom = 49,  $p < 0.001$ , CMIN/DF = 2.478, CFI = 0.950, GFI = 0.926, and RMR = 0.027 the model satisfies all model fit parameters (Path c). The standardised total effect of online security and online trust on behavioural purchase intention is 0.516 and r square is increased to 0.49. The standardised direct effect of online security on purchase intention is 0.019 ( $p < 0.001$ ) and the standardised indirect effect is 0.497 ( $p < 0.001$ ) which indicates the presence of mediation of online trust (Table 6). With this, condition three of the Barron and Kenny approach is also satisfied.

Table 6. Model fit parameters and Standardized Regression Estimates for H<sub>5</sub>

Model Fit Parameters				Standardized Regression Estimates						
Path	$\chi^2$	Df	$p$	CMIN/DF	CFI	GFI	RMR	Estimate	S.E.	C.R.
Path a	43.954	24	***	1.831	0.981	0.964	0.018	0.610	0.074	8.236
Path b	43.003	11	***	3.909	0.958	0.955	0.034	0.512	0.080	6.371
Path c	121.409	49	***	2.478	0.950	0.926	0.027	0.018	0.105	0.173

Note:  $\chi^2$  = Chi-square Df = Degrees of freedom; \*\*\* =  $p < 0.001$ . Source: Compiled by the researchers.

To check the type of mediation, now in the presence of mediator, the relationship between online security and purchase intention is to be identified. The relationship between online security and purchase intention in the presence of online trust is found to be insignificant (Beta = 0.018, S.E. = 0.105, C.R. = 0.173,  $p = 0.862$ ) (Table 7). Hence, online trust acts as a full mediator between online security and purchase intention.

Table 7. Checking mediating role of online trust on the relationship between online security and purchase intention (Hypothesis 5)

	Standardized Total Effects		Standardized Direct Effects		Standardized Indirect Effects	
	Online Security	Online Trust	Online Security	Online Trust	Online Security	Online Trust
Online Trust	0.727	0	0.727	0	0	0
Purchase Intention	0.516	0.684	0.019	0.684	0.497	0

Source: Compiled by the researchers.

Similarly, to test hypothesis six (H<sub>6</sub>), all three conditions stated according to Baron and Kenny (1986) are satisfied (Table 8). With Chi-square = 57.412, Degrees of freedom = 26,  $p <$

0.001, CMIN/DF = 2.208, CFI = 0.966, GFI = 0.951, and RMR = 0.024 the model satisfies all model fit parameters. Online trust regresses significantly on online privacy (path a).

With Chi-square = 26.738, Degrees of freedom = 13,  $p < 0.001$ , CMIN/DF = 2.057, CFI = 0.979, GFI = 0.971, and RMR = 0.023 the model satisfies all model fit parameters. Purchase intention regresses significantly on online privacy in absences of mediator. Hence, condition two of Baron and Kenny's Mediating Analysis approach is also satisfied.

With Chi-square = 118.148, Degrees of freedom = 51,  $p < 0.001$ , CMIN/DF = 2.317, CFI = 0.949, GFI = 0.926, and RMR = 0.026 the model satisfies all model fit parameters (Path c).

Table 8. Model fit parameters and Standardized Regression Estimates for H<sub>6</sub>

Model Fit Parameters				Standardized Regression Estimates						
Path	$\chi^2$	Df	$p$	CMIN/DF	CFI	GFI	RMR	Estimate	S.E.	C.R.
Path a	57.412	26	***	2.208	0.966	0.951	0.024	0.513	0.066	7.825
Path b	26.738	13	26.738	26.738	0.979	0.971	0.023	0.493	0.073	6.759
Path c	118.148	51	0.140	2.317	0.949	0.926	0.026	0.125	0.084	1.477

Note:  $\chi^2$  = Chi-square Df = Degrees of freedom, \*\*\* =  $p < 0.001$ . Source: Compiled by the researchers.

The standardised total effect of online privacy and online trust on purchase intention is 0.536 and r square is increased to 0.49. The standardised direct effect of online privacy on purchase intention is 0.137 ( $p < 0.001$ ) and the standardise indirect effect is 0.399 ( $p < 0.001$ ) which indicates presence of mediation of online trust (Table 9). With this, condition three of the Barron and Kenny approach is also satisfied.

To check the type of mediation, now in the presence of mediator, the relationship between online privacy and purchase intention is to be identified. The relationship between online privacy and purchase intention in the presence of online trust is found to be insignificant (Beta = 0.125, S.E. = 0.084, C.R. = 1.477,  $p > 0.001$ ) (Table 9). Hence, online trust acts as a full mediator between online privacy and purchase intention.

Table 9. Checking mediating role of online trust on the relationship between online privacy and purchase intention (hypothesis 6)

	Standardized Total Effects		Standardized Direct Effects		Standardized Indirect Effects	
	Online Privacy	Online Trust	Online Privacy	Online Trust	Online Privacy	Online Trust
Online Trust	0.66	0	0.66	0	0	0
Purchase Intention	0.536	0.605	0.137	0.605	0.399	0

Source: Compiled by the researchers.

Finally, with Chi-square = 58.327, Degrees of freedom = 19,  $p < 0.001$ , CMIN/DF = 3.070, CFI = 0.953, GFI = 0.948, RMSEA = 0.091, RMR = 0.029 the model satisfies all model



fit parameters (Table 10). Online trust regresses significantly on web app. Hence, condition one of Baron and Kenny's Mediating Analysis approach is satisfied. Additionally, with Chi-square = 18.721, Degrees of freedom = 8,  $p < 0.001$ , CMIN/DF = 18.721, CFI = 0.983, GFI = 0.976, and RMR = 0.016 the model satisfies all model fit parameters. Purchase intention regresses significantly on web app in absences of mediator. Hence, condition two of Baron and Kenny's Mediating Analysis approach is also satisfied. Lastly, with Chi-square = 110.664, Degrees of freedom = 41,  $p < 0.001$ , CMIN/DF = 2.699, CFI = 0.944, GFI = 0.930, and RMR = 0.026 the model satisfies all model fit parameters.

Table 10. Model fit parameters and Standardized Regression Estimates for hypotheses seven

Model fit parameters				Standardized Regression Estimates						
Path	$\chi^2$	Df	$p$	CMIN/DF	CFI	GFI	RMR	Estimate	S.E.	C.R.
Path a	58.327	19	***	3.070	0.953	0.948	0.029	0.677	0.123	5.515
Path b	18.721	8	***	0.016	0.983	0.976	0.016	1.007	0.160	6.312
Path c	110.664	41	***	***	0.944	0.930	0.026	0.517	0.127	4.063

Note:  $\chi^2$  = Chi-square Df = Degrees of freedom, \*\*\* =  $p < 0.001$ . Source: Compiled by the researchers.

The standardised total effect of web app and online trust on purchase intention is 0.593 and r square is increased to 0.57 (Table 10). The standardised direct effect of web app on purchase intention is 0.319 ( $p < 0.001$ ) and the standardised indirect effect is 0.274 ( $p < 0.001$ ) which indicates presence of mediation of online trust. With this, condition three of the Barron and Kenny approach is also satisfied. To check the type of mediation, now in the presence of mediator, the relationship of website appearance and purchase intention is to be identified. The relationship between website appearance and purchase intention in the presence of online trust is found to be significant (Beta = 0.517, S.E. = 0.127, C.R. = 4.063,  $p < 0.001$ ) (Table 11). Hence, online trust acts as a partial mediator between web app and purchase intention.

Table 11. Checking mediating role of online trust on the relationship between website appearance and purchase intention ( $H_7$ )

	Standardized Total Effects		Standardized Direct Effects		Standardized Indirect Effects	
	Web Appearance	Online Trust	Web Appearance	Online Trust	Web Appearance	Online Trust
Online Trust	0.508	0	0.508	0	0	0
Purchase Intention	0.593	0.54	0.319	0.54	0.274	0

Source: Compiled by the researchers.

## CONCLUSIONS

This study is an attempt towards validating the importance of online security, online privacy, and website appearance for Generation Z in developing online trust towards e-

commerce websites and eventually influencing the intention to purchase. The analyzed results show the resultant impact of respondents' beliefs about proffered security and privacy for online trust towards the respective e-commerce websites. This is consistent with the findings of Al-Adwan, Al-Debei, and Dwivedi, (2022); Al-Adwan and Al-Horani, (2019); Salimon et al. (2015); Forsythe and Shi, 2003; D. J. Kim et al., 2008; and Weisberg et al.(2011). Where the e-commerce platform is trustworthy, consumers tend to share personal, financial, and behavioral information with lesser concern and feel motivated to use the services.

Security and privacy features are considered as important issues for e-commerce design as users are more interested in dealing with it when they perceive that the information provided during the transactions is secure and no other party will have access to it. If the users have less worries about unauthorized use of access to their personal and financial information by any other party, then they will tend to develop higher trust in the e-commerce system, and this will add to the higher intention to purchase (Roca et al., 2009). Therefore, e-commerce companies should work to improve their web security features to enhance the users' online trust.

Users' positive perceptions of the security strengthening tactics leads to their perception of trust towards the e-commerce mechanism of the company (Chellappa and Pavlou 2002). Companies can also educate their customers on different ways of keeping their information safe and ensuring their online security. Regularly asking users to change their unique login credentials is another way of contributing towards a safer digital environment. Asking users to keep their devices safe by adding any kind of firewall, antivirus, or any other appropriate method helps protect them from online threats. Hackers and phishers also operate through duplicate websites having the same name with a small change in spelling or domain, so companies can create awareness among users about this tactic and appeal for using the correct website of the company.

The results of this study show that the appearance of the e-commerce website also plays a significant role and is found to be a significant predictor of the level of online trust towards the website. The impression of e-commerce websites' visual design, appeal, ease of use, and space utilization helped in developing the trust of the respondents. This confirms the findings of Gafen et al., (2004), Cyr et al., (2010), and Harrison McKnight et al. (2002). E-commerce website designers and developers should note that the appearance of the website should be planned in a way which ensures trust among the users. The audience expects a simple, intuitive, and usable user interface which minimize cluttering and displays clear information. Such designs also facilitate smooth and easy signups, convenient searches, and speedy decision-

making. A website is the face of any e-commerce business; it provides to its users the visuals of its products and services and its supports. In the minds of users, websites create first impressions which may last for a long time. The experiences of the users with websites will decide their future course of association among the available choices. A design which seems professional to visitors, whereby special visual and aesthetical aspects account for lasting impressions, in turn triggers trust development. Along with graphical attributes (aesthetics, color combination, fonts combinations, highlights, attractiveness), structural attributes are also very important for the effective and appealing appearance of the website. Structural appearance covers themes such as the placement of icons and applications, navigation facilities, search facilities, ease of accessing, autosave, help links, etc.). Our study guides sellers to maintain users' trust by focusing on the continuous improvement in the appearance of its website so that the listed products are increasingly believed to deliver desired performances resulting in the development of trust and positive intention to purchase. E-commerce businesses must ensure the good quality of website design and comply with users' needs and perceptions. Many times, it is observed that the user does not get sufficient information and awareness from the e-commerce website appearance; thus, the business is expected to maintain and improve the design quality of the website (Priscillia et al., 2021). Users visit an e-commerce website with different motives and one of them is to find information about the products, services, reviews, recommendations, prices, and policies of the company. Every business website should provide complete, useful, and reliable information with the demonstration of elegance, usefulness, accuracy, and diversity (Yang et. al., 2005)

Our study also confirms the importance of online trust in developing the purchase intention towards an e-commerce website. Trust of the users has also been defined as the willingness to be vulnerable depending on the confidence held towards the positive expectations of other's behavior and intentions (Rousseau et al., 1998). Higher trust perception leads to higher intention to purchase; users are more likely to transact online when they have trust in the e-commerce company and their website (Ganguly et al., 2009; Weisberg et al., 2011). Trust is an important determinant for supporting the e-commerce transactions and an important predictor of a user's intention to purchase through e-commerce websites (Think et al., 2017). When users feel a sense of trust towards an e-commerce website, this can automatically trigger their intention to buy from the website. This mediated pathway presents online trust as a mediator which helps translate online security and online privacy into purchase intention. In the first instance, a facility to ensure online security and privacy offered to the

users exerts positive influence on online trust and in the second instance the developed trust influences the intention to make a purchase. Online trust is further found to have a partial mediation relation between website appearance and purchase intention.

### **Strategic Implication**

The COVID-19 pandemic added to the urgency to go online. This is the need of the hour, even for an offline business, it is time to have presence over the internet. However, this also came as an opportunity for spammers, hackers, fraudsters, and digital thieves. Thus, if any e-commerce business naively thinks that their website is immune to any security concern, it can prove to be a big mistake. It is not only putting the e-commerce business at risk but is also compromising the security and privacy of the customers who believed in you and your claims. This present study helps demonstrate the significance of online security, online privacy, and the appearance of e-commerce websites for a young generation (Generation Z) in facilitating online trust, especially during coronavirus times. It also confirms the positive significant relationship between online trust and intention to purchase through e-commerce websites. The findings strongly endorse the ever-growing need of a system to ensure the privacy of the information (personal, monetary, and preferences). Not only during the ongoing pandemic, for always privacy protection systems need to be reviewed and improved from time to time as the cyber world is continuously under the attack of cyber hackers. Similarly, online security is another important area which needs regular monitoring by e-commerce websites. This study confirms the findings of Flavián and Guinalú (2006) that trust can be enhanced especially by developing a sense of security in consumers who use the systems adopted by an e-commerce website. E-commerce marketers and technical executives must invest not only towards the development of security systems, but also on continuous efforts for the minimization of risks involving online transactions and data theft.

E-commerce players are now practicing strict protocols for ensuring the security and privacy of the users. Integrity pledge is a must for e-commerce businesses, where any information is not allowed to be modified or even seen by any third party at any stage of operation. A business usually has contacts with many third parties for other processes. Strict firewalls are used to keep related information out of access of any third party. Non-Repudiation policies are followed by many e-commerce businesses. A 24 × 7 and 365-day availability of grievance handling mechanisms globally is also a common practice these days. This study also throws light on the significance of the appearance of a website and its qualities. When the whole

world is experiencing social distancing and lockdowns, websites emerge as the one of the most important windows to investigate the commercial world. A website is the mirror of the business, and its appearance is also found to have a significant impact on online trust, which means that respondents view the overall design, web architecture, user interface, placement of icons, colors combinations, etc., as having some impact on forming online trust towards the respective e-commerce website. This confirms the previous studies by Gefen et al. (2004), Cyr et al., (2010), and Harrison McKnight et al., (2002). A website is one of the main mediums for direct interaction and engagement with consumers, so if it is well designed and ensures ease of use, then it contributes towards forming strong online trust among users. The theoretical significance of this study lies in its timing. The COVID-19 pandemic has pushed towards further digitalization and the mass adoption and development of e-commerce (Santo and Marques, 2022). Issues related to security and privacy have always been significant for developing trust among users, but the pandemic has made it mandatory more than at any time during the past. It is about securing the personal and private data of the end users from getting misused by fraudsters. E-commerce businesses now need to be more vigilant than ever as not all participants and vendors they come across are legitimate (Ma and McKinnon, 2022). Fraudsters are now more equipped and creative to adapt to the market (Boman and Gallupe, 2020). The high number and frequency of e-commerce transactions forced by the policies enacted to tackle the coronavirus pandemic has surely made it significantly riskier (Karpoff, 2020). Website appearance is an understudied concept when studied with reference to online trust. In today's scenario, a website is regarded as the first impression of any business. It becomes even more important when the business is an e-commerce business. The appearance and design of a website gives an idea about the business and the quality of service and eventually leads to building trust (Cyr et al., 2010; S. Kim and Stoel, 2004b, 2004a; Harrison McKnight et al., 2002). Marketers and website developers can conduct regular surveys and studies to make sure that users express their feedback and experience with the current state of the site to facilitate its further improvement. During extraordinary conditions, like what we have seen in the pandemic where people were dealing with emotional challenges, anxiety, stress, and many more psychological issues, they become easier targets for digital thieves (Ma and McKinnon, 2022). Under such scenarios, developing trust through website appearance is the second most significant finding in the study ( $\beta = 0.35, p < 0.001$ ). Ensuring online security and privacy are still significant for developing trust among e-commerce users. This study endorses the act of spending resources towards the development and maintenance of a website and its

appearance, such as the consistent use of colors, navigation, icons placement, logos, design, and symbols. Furthermore, while adopting the above suggestions, due care must be given to the size of the website, i.e., it should be easy to open, and heavy websites which often lead to the time-out error should be avoided. E-commerce companies have become much more concerned with website appearance over the years. Now, they are also focusing on making efforts to develop the mobile responsiveness of their model. Businesses are trying to develop a customizable model of a website, as aesthetics and appearance is defined as a subjective concept. Customizability is giving new dimensions to website appearance. Easy User Interface (UI) has also become a point of brainstorming for businesses. Companies have started thinking about website appearance differently based on B2B and B2C orientation. E-commerce businesses know that building a better looking website is equivalent to building the trust of the visitors. An important outcome of a nurtured trust is to entice a user to make a purchase. Securing an intention to purchase has always been a vital act for the survival of any business. Our results confirm the significant impact of online trust on the purchase intention. When users have trust in the e-commerce website, it shows their feeling and understanding that the seller is not going to deceive or claim unjustified gains from them. Our findings were consistent with the findings of Wang et al. (2003), Gafen et al. (2004), and Grabner-Kräuter and Kaluscha, (2003). The findings of this study highlight the importance of online security, online privacy, and the appearance of e-commerce websites for a young generation (Gen-Z). This generation is regarded as a tech-savvy generation, who spend much of their time on the world wide web using many internet-based applications in their day-to-day life. Many e-commerce vendors are targeting this generation with products exclusively designed for them, so the suggestions of this study are going to be a relevant subject for them.

### **Limitations and Future Scope**

Admittedly, this study is not free from limitations. The cross-sectional nature of this study makes it difficult for making inferences about causal relationships so new studies can adopt and check the utility of a longitudinal approach in this area. Furthermore, the data collected using convenience sampling had all young generation respondents, mostly college/university students. This current study takes only three antecedents of online trust with reference to a young generation; an exploratory study is needed here to find out new possible antecedents of developing online trust. Moreover, the appearance of the website is altogether a vast area to investigate for further development; very limited dimensions of the appearance of

e-commerce websites are covered in this study. The website is a multidimensional concept; appearance is just one side of website design so future researchers can go into detail with this aspect. Content quality of the website, TAM model, response time of the website, functionality, creativity, profile management, etc., can all be explored with reference to this website design concept. Some other variables may moderate the relationship between website appearance and intention to purchase. Separate space for discussion, product review, and ratings for users is also a new trend in e-commerce website design. Future researchers can explore this electronic word of mouth space as it also plays an important role in shaping the brand relationships and purchase intention of the users (Habib et al., 2021; Siddiqui et al., 2021). Demographic factors may play an important role in the development of trust and consumer behavior towards e-commerce websites, which is ignored in this study. Especially in India where women have started joining the workforce, in the future they are going to play a major role in the e-commerce world. It would be interesting to explore the response of the e-commerce players to this social change. Trust has also been explored by researchers in different dimensions, such as trust in the e-commerce website, trust in the vendor of the product, and trust in the shipping partner. Future researchers can also go in this direction.

## REFERENCES

1. Al Abri, D.; McGill, T.; Dixon, M. Examining the Impact of E-privacy Risk Concerns on Citizens' Intentions to Use E-government Services: An Oman Perspective. *J. Inf. Priv. Secur.* **2009**, *5*, 3–26. <https://doi.org/10.1080/15536548.2009.10855861>
2. Al-Adwan, A.S.; Alrousan, M.K.; Yaseen, H.; Alkufahy, A.M.; Alsoud, M. Boosting Online Purchase Intention in High-Uncertainty-Avoidance Societies: A Signaling Theory Approach. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 136. <https://doi.org/10.3390/joitmc8030136>
3. Al-Adwan, A.S.; Al-Debei, M.M.; Dwivedi, Y.K. E-commerce in high uncertainty avoidance cultures: The driving forces of repurchase and word-of-mouth intentions. *Technol. Soc.* **2022**, *71*, 102083. <https://doi.org/10.1016/j.techsoc.2022.102083>
4. Al-Adwan, A.S.; Al-Horani, M.A. Boosting customer e-loyalty: An extended scale of online service quality. *Information* **2019**, *10*, 380. <https://doi.org/10.3390/info10120380>
5. Barclay, D.; Thompson, R.; dan Higgins, C. The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use of an illustration. *Technol. Stud.* **1995**, *2*, 285–309. <https://doi.org/10.1017/CBO9781107415324.004>
6. Baumgartner, H.; Homburg, C. Applications of Structural Equation Modeling in Marketing and Consumer Research: A review. *Int. J. Res. Mark.* **1996**, *13*, 139–161.

7. BCG; Bain & Company; Morgan Stanley. (1 July 2020). Market Size of E-Commerce Industry across India from 2014 to 2018, with Forecasts Until 2027. Available online: [www.statista.com: https://www.statista.com/statistics/792047/india-e-commerce-market-size/](https://www.statista.com/statistics/792047/india-e-commerce-market-size/) (accessed on 19 March 2021).
8. Bentler, P.M. Comparative fit indexes in structural models. *Psychol. Bull.* **1990**, *107*, 238–246. <https://doi.org/10.1037/0033-2909.107.2.238>
9. Bhattacharjee, A. Bhattacharjee continuance: *MIS Q.* **2011**, *25*, 351–370.
10. Boman, J.H.; Gallupe, O. Has COVID-19 changed crime? Crime rates in the United States during the pandemic. *Am. J. Crim. Justice* **2020**, *45*, 537–545.
11. Brotheridge, C.M.; Zyglidopoulos, D. Selling shoes through gendered emotional displays. *Int. J. Work. Organ. Emot.* **2006**, *1*, 189–203. <https://doi.org/10.1504/IJWOE.2006.010787>.
12. Chellappa, R.K.; Pavlou, P.A. Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logist. Inf. Manag.* **2002**, *15*, 358–368. <https://doi.org/10.1108/09576050210447046>
13. Chen, Y.; Friedman, R.; Tony Simons. Article Information—Home Article Information—Home. *Manag. Audit. J.* **2014**, *28*, 2–3.
14. Cyr, C.; Euser, E.M.; Bakermans-Kranenburg, M.J.; Van Ijzendoorn, M.H. Attachment security and disorganization in maltreating and high-risk families: A series of meta-analyses. *Dev. Psychopathol.* **2010**, *22*, 87–108. <https://doi.org/10.1017/S0954579409990289>
15. Coppola, D. (19 February 2021). E-Commerce Worldwide—Statistics & Facts. Available online: <https://www.statista.com/topics/871/online-shopping/> (accessed on March 2021).
16. Dibb, J.C. Consumer Trust in the Online Retail Context: Exploring the Antecedents and Consequences. *Psychol. Mark.* **2010**, *24*, 323–346. <https://doi.org/10.1002/mar.20334>.
17. Donthu, N.; Gustafsson, A. Effects of COVID-19 on business and research. *J. Bus. Res.* **2020**, *117*, 284–289.
18. Field, A.P. *Discovering Statistics Using SPSS: (and Sex and Drugs and Rock 'n' Roll)*; SAGE Publications: Los Angeles, CA, USA; Thousand Oaks, CA, USA, 2009.
19. Flavián, C.; Guinaliú, M. Consumer trust, perceived security, and privacy policy: Three basic elements of loyalty to a web site. *Ind. Manag. Data Syst.* **2006**, *106*, 601–620. <https://doi.org/10.1108/02635570610666403>
20. Forsythe, S.M.; Shi, B. Consumer patronage and risk perceptions in Internet shopping. *J. Bus. Res.* **2003**, *56*, 867–875. [https://doi.org/10.1016/S0148-2963\(01\)00273-9](https://doi.org/10.1016/S0148-2963(01)00273-9)
21. Ganguly, B.; Dash, S.B.; Cyr, D. Website characteristics, Trust and purchase intention in online stores:-An Empirical study in the Indian context. *J. Inf. Sci. Technol.* **2009**, *6*.



22. Gefen, D.; Straub, D.W. Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega* **2004**, *32*, 407–424. <https://doi.org/10.1016/j.omega.2004.01.006>
23. Goh, E.; Lee, C. A workforce to be reckoned with: The emerging pivotal Generation Z hospitality workforce. *Int. J. Hosp. Manag.* **2018**, *73*, 20–28. <https://doi.org/10.1016/j.ijhm.2018.01.016>
24. Grabner-Kräuter, S.; Kaluscha, E.A. Empirical research in on-line trust: A review and critical assessment. *Int. J. Hum. Comput. Stud.* **2003**, *58*, 783–812. [https://doi.org/10.1016/S1071-5819\(03\)00043-0](https://doi.org/10.1016/S1071-5819(03)00043-0)
25. Habib, S.; Hamadneh, N.N.; Khan, M.A. Influence of electronic word of mouth (Ewom) and relationship marketing on brand resonance: A mediation analysis. *Sustainability* **2021**, *13*, 6833. <https://doi.org/10.3390/su13126833>
26. Hair, J.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*, 7th ed.; Pearson Education International: Upper Saddle River, NJ, USA, 2010.
27. Hair, J., Jr.; Hult, G.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed.; Sage Publications: Thousand Oaks, CA, USA, 2016
28. Harrison McKnight, D.; Choudhury, V.; Kacmar, C. The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *J. Strateg. Inf. Syst.* **2002**, *11*, 297–323. [https://doi.org/10.1016/S0963-8687\(02\)00020-3](https://doi.org/10.1016/S0963-8687(02)00020-3)
29. Hong, I.B.; Cho, H. The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. *Int. J. Inf. Manag.* **2011**, *31*, 469–479. <https://doi.org/10.1016/j.ijinfomgt.2011.02.001>
30. Hsiao, K.L.; Lin, J.C.C.; Wang, X.Y.; Lu, H.P.; Yu, H. Antecedents and consequences of trust in online product recommendations: An empirical study in social shopping. *Online Inf. Rev.* **2010**, *34*, 935–953. <https://doi.org/10.1108/14684521011099414>
31. Karpoff, J.M. The future of financial fraud. *J. Corp. Financ.* **2021**, *66*, 101694.
32. Kauffman, R.J.; Lai, H.; Lin, H.C. Consumer adoption of group-buying auctions: An experimental study. *Inf. Technol. Manag.* **2010**, *11*, 191–211. <https://doi.org/10.1007/s10799-010-0068-z>
33. Khan, M.A. Netizens' Perspective towards Electronic Money and Its Essence in the Virtual Economy: An Empirical Analysis with Special Reference to Delhi-NCR, India. *Complexity* **2021**, *2021*, 1–18. <https://doi.org/10.1155/2021/7772929>
34. Kim, D.J.; Ferrin, D.L.; Rao, H.R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst.* **2008**, *44*, 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>

35. Kim, D.J.; Yim, M.S.; Sugumaran, V.; Rao, H.R. Web assurance seal services, trust, and consumers' concerns: An investigation of e-commerce transaction intentions across two nations. *Eur. J. Inf. Syst.* **2016**, *25*, 252–273. <https://doi.org/10.1057/ejis.2015.16>
36. Kim, M.S.; Ahn, J.H. Management of trust in the e-marketplace: The role of the buyer's experience in building trust. *J. Inf. Technol.* **2007**, *22*, 119–132. <https://doi.org/10.1057/palgrave.jit.2000095>
37. Kim, S.; Stoel, L. Apparel retailers: Website quality dimensions and satisfaction. *J. Retail. Consum. Serv.* **2004a**, *11*, 109–117. [https://doi.org/10.1016/S0969-6989\(03\)00010-9](https://doi.org/10.1016/S0969-6989(03)00010-9)
38. Kim, S.; Stoel, L. Dimensional hierarchy of retail website quality. *Inf. Manag.* **2004b**, *41*, 619–633. <https://doi.org/10.1016/j.im.2003.07.002>
39. Kim, Y.; Peterson, R.A. A Meta-analysis of Online Trust Relationships in E-commerce. *J. Interact. Mark.* **2017**, *38*, 44–54. <https://doi.org/10.1016/j.intmar.2017.01.001>
40. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248.
41. Lee, S.A. Coronavirus Anxiety Scale: A brief mental health screener for COVID-19 related anxiety. *Death Stud.* **2020**, *44*, 393–401. <https://doi.org/10.1080/07481187.2020.1748481>
42. Lian, J.W.; Lin, T.M. Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Comput. Hum. Behav.* **2008**, *24*, 48–65. <https://doi.org/10.1016/j.chb.2007.01.002>
43. Lim, N. Consumers' perceived risk: Sources versus consequences. *Electron. Commer. Res. Appl.* **2003**, *2*, 216–228. [https://doi.org/10.1016/S1567-4223\(03\)00025-5](https://doi.org/10.1016/S1567-4223(03)00025-5)
44. Lu, Y.; Zhao, L.; Wang, B. From virtual community members to C2C e-commerce buyers: Trust in virtual communities and its effect on consumers' purchase intention. *Electron. Commer. Res. Appl.* **2010**, *9*, 346–360. <https://doi.org/10.1016/j.elerap.2009.07.003>
45. Ma, K.W.F.; McKinnon, T. COVID-19 and cyber fraud: Emerging threats during the pandemic. *J. Financ. Crime* **2022**, *29*, 433–446. <https://doi.org/10.1108/JFC-01-2021-0016>
46. Mael, F.; Ashforth, B.E. Alumni and their alma mater: A partial test of the reformulated model of organizational identification. *J. Organ. Behav.* **1992**, *13*, 103–123. <https://doi.org/10.1002/job.4030130202>
47. Malhotra, N.; Hall, J.; Shaw, M.; Oppenheim, P. *Marketing Research: An Applied Orientatio*; Deakin University: Melbourne, Australia, 2006.
48. Martin, J.; Mortimer, G.; Andrews, L. Re-examining online customer experience to include purchase frequency and perceived risk. *J. Retail. Consum. Serv.* **2015**, *25*, 81–95. <https://doi.org/10.1016/j.jretconser.2015.03.008>

49. Mathieson, K. Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Inf. Syst. Res.* **1991**, 2, 173–191. <https://doi.org/10.1287/isre.2.3.173>
50. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An integrative model of organizational trust. *Acad. Manag. Rev.* **1995**, 20, 709–734.
51. Naidoo, R. A multi-level influence model of COVID-19 themed cybercrime. *Eur. J. Inf. Syst.* **2020**, 29, 306–321. <https://doi.org/10.1080/0960085X.2020.1771222>
52. Netemeyer, R.G.; Bearden, W.O.; Sharma, S. *Scaling Procedures: Issues and Applications*; Sage Publications: Thousand Oaks, CA, USA, 2003.
53. Pabian, A.; Pabian, B.; Reformat, B. E-customer security as a social value in the sphere of sustainability. *Sustainability* **2020**, 12, 590. <https://doi.org/10.3390/su122410590>.
54. Pavlou, P.A. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *Int. J. Electron. Commer.* **2003**, 7, 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
55. Pavlou, P.A.; Gefen, D. Building effective online marketplaces with institution-based trust. *Inf. Syst. Res.* **2004**, 15, 37–59. <https://doi.org/10.1287/isre.1040.0015>
56. Pavlou, P.A.; Huigang, L.; Yajiong, X. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Q. Manag. Inf. Syst.* **2007**, 31, 105–135. <https://doi.org/10.2307/25148783> .
57. Pennington, R.; Dixon Wilcox, H.; Grover, V. The Role of System Trust in Business-to-Consumer Transactions. *J. Manag. Inf. Syst.* **2003**, 20, 197–226. <https://doi.org/10.1080/07421222.2003.11045777> .
58. Ponirir; Scott, D.; Von Der Heidt, T. *E-Loyalty: Its Antecedents, Implications and Differences between Developed and Developing Countries*; Springer: Cham, Switzerland, 2015; pp. 77–82. [https://doi.org/10.1007/978-3-319-18696-2\\_29](https://doi.org/10.1007/978-3-319-18696-2_29) .
59. Quach, S.; Thaichon, P. From connoisseur luxury to mass luxury: Value co-creation and co-destruction in the online environment. *J. Bus. Res.* **2017**, 81, 163–172. <https://doi.org/10.1016/j.jbusres.2017.06.015> .
60. Roca, J.C.; García, J.J.; de la Vega, J.J. The importance of perceived trust, security, and privacy in online trading systems. *Inf. Manag. Comput. Secur.* **2009**, 17, 96–113. <https://doi.org/10.1108/09685220910963983> .
61. Rodrigues, V.F.; Policarpo, L.M.; da Silveira, D.E.; Righi, R.d.R.; da Costa, C.A.; Barbosa, J.L.V.; Antunes, R.S.; Scorsatto, R.; Arcot, T. Fraud detection and prevention in e-commerce: A systematic literature review. *Electron. Commer. Res. Appl.* **2022**, 56, 101207. <https://doi.org/10.1016/j.elerap.2022.101207>.
62. Rousseau, D.M.; Sitkin, S.B.; Burt, R.S.; Camerer, C. Not so different after all: A cross-discipline view of trust. *Acad. Manag. Rev.* **1998**, 23, 393–404. <https://doi.org/10.5465/AMR.1998.926617>.

63. Salam, A.F.; Lyer, L.; Palvia, P.; Singh, R. Trust in e-commerce. *Commun. ACM* **2005**, *48*, 72–77. <https://doi.org/10.1145/1042091.1042093>
64. Salimon, M.G.; Yusoff, R.Z.; Mokhtar, S.S. The impact of perceived security on e-trust, e-satisfaction and adoption of electronic banking in Nigeria: A conceptual review. *J. Bus. Manag.* **2015**, *17*, 64–69. <https://doi.org/10.9790/487X-171016469>
65. Keelery, S. (7 July 2020). INTERNET Usage in India—Statistics & Facts. Available online: <https://www.statista.com/topics/2157/internet-usage-in-india/> (accessed on 19 March 2021).
66. Santo, P.E.; Marques, A.M.A. Determinants of the online purchase intention: Hedonic motivations, prices, information and trust. *Balt. J. Manag.* **2022**, *17*, 56–71. <https://doi.org/10.1108/BJM-04-2021-0140>
67. Shen, K.N.; Khalifa, M. System design effects on online impulse buying. *Internet Res.* **2012**, *22*, 396–425. <https://doi.org/10.1108/10662241211250962> .
68. Shim, S.; Eastlick, M.A.; Lotz, S.L.; Warrington, P. An online pre-purchase intentions model. *J. Retail.* **2001**, *77*, 397–416. [https://doi.org/10.1016/s0022-4359\(01\)00051-3](https://doi.org/10.1016/s0022-4359(01)00051-3) .
69. Shu, W.; Chuang, Y.H. The perceived benefits of six-degree-separation social networks. *Internet Res.* **2011**, *21*, 26–45. <https://doi.org/10.1108/10662241111104866> .
70. Siddiqui, M.S.; Siddiqui, U.A.; Khan, M.A.; Alkandi, I.G.; Saxena, A.K.; Siddiqui, J.H. Creating electronic word of mouth credibility through social networking sites and determining its impact on brand image and online purchase intentions in India. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 1008–1024. <https://doi.org/10.3390/jtaer16040057> .
71. Sin, S.S.; Nor, K.M.; Al-Agaga, A.M. Factors Affecting Malaysian young consumers' online purchase intention in social media websites. *Procedia Soc. Behav. Sci.* **2012**, *40*, 326–333. <https://doi.org/10.1016/j.sbspro.2012.03.195> .
72. Steiger, J. Understanding the limitations of global fit assessment in structural equation modeling. *Personal. Individ. Differ.* **2007**, *42*, 893–898 .
73. Szymanski, D.M.; Hise, R.T. E-satisfaction: An initial examination. *J. Retail.* **2000**, *76*, 309–322. [https://doi.org/10.1016/S0022-4359\(00\)00035-X](https://doi.org/10.1016/S0022-4359(00)00035-X) .
74. Thin, N.H.T.; Van Huy, L.; Son, N.T. The Impact of Website Service Quality on Customer Trust and Purchase Intentions in the Hotel: Theoretical Approach. *Int. J. Appl. Bus. Econ. Res.* **2017**, *15*, 479–498.
75. Tsvetovat, M.; Sycara, K. Customer coalitions in the electronic marketplace. In Proceedings of the International Conference on Autonomous Agents, Barcelona, Spain, 3–7 June 2000; pp. 263–264. <https://doi.org/10.1145/336595.337479> .
76. Verma, P. The Effect of Brand Engagement and Brand Love upon Overall Brand Equity and Purchase Intention: A Moderated –Mediated Model. *J. Promot. Manag.* **2021**, *27*, 103–132. <https://doi.org/10.1080/10496491.2020.1809591> .

77. Vinerean, S.; Cetina, I.; Dumitrescu, L.; Tichindelean, M. The Effects of Social Media Marketing on Online Consumer Behavior. *Int. J. Bus. Manag.* **2013**, *8*, 66–79. <https://doi.org/10.5539/ijbm.v8n14p66> .
78. Wang, Y.S.; Wang, Y.M.; Lin, H.H.; Tang, T.I. Determinants of user acceptance of Internet banking: An empirical study. *Int. J. Serv. Ind. Manag.* **2003**, *14*, 501–519. <https://doi.org/10.1108/09564230310500192> .
79. Weisberg, J.; Te'eni, D.; Arman, L. Past purchase and intention to purchase in e-commerce: The mediation of social presence and trust. *Internet Res.* **2011**, *21*, 82–96. <https://doi.org/10.1108/10662241111104893> .
80. Wheaton, B.; Muthen, B.; Alwin, D.F.; Summers, G. Assessing Reliability and Stability in Panel Models. *Sociol. Methodol.* **1977**, *8*, 84–136.
81. Wronka, C. Impact of COVID-19 on financial institutions: Navigating the global emerging patterns of financial crime. *J. Financ. Crime* **2022**, *29*, 476–490. <https://doi.org/10.1108/JFC-03-2021-0073> .
82. Wu, I.-L.; Chen, J.-L. An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study. *Int. J. Hum. Comput. Stud.* **2005**, *62*, 784–808. <https://doi.org/10.1016/j.ijhcs.2005.03.003>.
83. Yang, Y.; Hu, Y.; Chen, J. A web trust-inducing model for e-commerce and empirical research. In Proceedings of the 7th International Conference on Electronic Commerce, Xi'an, China, 15–17 August 2005; pp. 188–194. <https://doi.org/10.1145/1089551.1089589> .
84. Yousafzai, S.Y.; Pallister, J.G.; Foxall, G.R. A proposed model of e-trust for electronic banking. *Technovation* **2003**, *23*, 847–860. [https://doi.org/10.1016/S0166-4972\(03\)00130-5](https://doi.org/10.1016/S0166-4972(03)00130-5) .
85. Zimmer, J.C.; Arsal, R.E.; Al-Marzouq, M.; Grover, V. Investigating online information disclosure: Effects of information relevance, trust, and risk. *Inf. Manag.* **2010**, *47*, 115–123. <https://doi.org/10.1016/j.im.2009.12.003> .