



---

## EXPLORING ONLINE SHOPPING SAFETY PERCEPTIONS IN DEVELOPING NATIONS: A LITERATURE REVIEW

ABU DARDA<sup>1</sup> 

SUDAY KUMER GHOSH<sup>2</sup> 

RONY BARUA<sup>3</sup> 

MST. FATEMA KHATUN<sup>4</sup> 

### ABSTRACT

The research paper explores the Online shopping safety as it becomes a part and parcel in individual's daily life with the rapid development of e-commerce. From buying convenience to logistics support, from product quality to customers service, these factors shape the customer satisfaction and loyalty towards online shopping. This study aims to explore the online shopping safety during 2020-2024 and also analyze the research gap through the systematic literature review. The research finding also suggest the future research according to the study. In this study, a systematic literature review was employed involving the search for the key word "online shopping safety" "online purchase intention" "online shopping risk" and "e-commerce experience" within the titles, abstracts and keyword of publication in the database. This systematic review contributes to the arena by offering in depth insight to the businessman and government stakeholder so that they can apply effective strategy for the online shopping safety and it will maximize the relationship between the ultimate consumer and businessman.

### KEYWORDS

Online shopping safety, e-commerce risk, consumer trust, digital infrastructure, online purchase intention, shopping behavior, PRISMA systematic review, developing nations, online transaction security, M-commerce, F-commerce, digital literacy, risk mitigation, e-commerce growth, COVID-19 trends.

---

<sup>1</sup> Post Graduate Researcher, Department of Marketing, University of Rajshahi, Bangladesh, Email: a.7darda@gmail.com, ORCID ID: 0009-0005-7542-0645

<sup>2</sup> Post Graduate Researcher, Department of Computer Science and Engineering (CSE), United International University, ORCID: 0009-0007-8536-2404

<sup>3</sup> Postgraduate Researcher, Department of Computer Science and Engineering, Daffodil International University, ORCID: 0009-0006-0950-8566

<sup>4</sup> Post Graduate Researcher, Department of Economics, Jagannath University, Bangladesh, ORCID ID: 0009-0009-9886-861X

## INTRODUCTION

At the first stage of COVID-19 people try to avoid physical store and minimize their exposure to the corona virus, the pandemic has increased the demand of online shopping and home delivery services of product (T. Ahmed, 2024). Online buying reduces physical frequency to the customers and among them women prefer online shopping then men because the roads of Dhaka is congested are not suitable for women (Enam et al., 2024). In fact, people who are living in the remote area and have poor transportation access can engage in online buying more (Enam et al., 2024).

On the other hand, there are many malfunctions in online shopping such as vulnerable website, poor quality of product, delay in delivery and security issue have been recognized as a significant hindrance for online shopping safety. In spite of having challenges, online shopping has many opportunities with the investment of digital infrastructure and developing new business model, additionally an effort should be applied enhancing the digital literacy (T. Ahmed, 2024).

Online shopping behavior are negatively influenced by perceived risk such as financial risk product risk, convenience risk and return risk but financial risk is less significant because of cash on delivery payment (T. Nguyen, 2024).

In spite of embracing opportunities presented by online shopping and considering the challenges. Government can build a strong and sustainable online shopping ecosystem that provides benefit from business man to ultimate customer and its economy as a whole. The Bangladesh government and concerned authorities like ministry of commerce should concern on online shopping, build digital infrastructure, ensure reliable e-commerce site and make a collaboration with the stakeholders to solve the issue of online shopping.

## BACKGROUND OF THE STUDY

With the influence of world wide web (WWW), people's views and action has tremendously change and they have already started buying their product from online platform. Mobile commerce (M-Commerce) and Facebook commerce (F-Commerce) are acquiring huge popularity in today's business world (Hossain & Jawad, 2022). Bangladesh has witnessed a surge in online shopping tendency in 2020 for lockdown COVID-19 and it has increased by 70% compared to the last year (Enam et al., 2024). According to (E-Cab, 2024), there are 2759 e-Commerce platforms in Bangladesh of which 1% large business , 4% Medium and 95% Small business.

Aside from electronic commerce, Bangladesh has witnessed a social media based business like F-commerce are rising rapidly (Hossain & Jawad, 2022). 300,000 Facebook business page are now present in the e commerce market place and 70% of the business page owners are women (Seddique Ul Huque Sazzad, 2023).

According to (T. Ahmed, 2024) some challenges were found including that almost 80% respondent faced difficulties unreliable websites, 68.5% complex payment system, 75% delay in delivery and 60% fraud activities. According to daily star (Report Business Star, 2023) E-orange, E-vally, Alesha mart raised their fund by embezzlement of consumer's money, on the other hand government set up an online complain box which act as a bridge between the customer, regulators agency and the e-commerce stakeholders.

## LITERATURE REVIEW

Online shopping safety refers to the measures and practices implemented to protect consumers and their information throughout the online purchasing process. This includes ensuring the security of financial transactions, protecting personal data from unauthorized access, verifying the authenticity and quality of products, preventing fraud, and maintaining a secure online environment to foster trust and confidence in e-commerce platforms. It

encompasses a broad range of aspects, from technological safeguards to regulatory compliance and user education.

From sensitivity to safety and secrecy issues in the online shopping is a key factor for manipulating digital consumer behavior, besides that, gaining popularity of online shopping and m-commerce influence customer behavior (Efendioğlu, 2024). COVID-19 has brought opportunity for the e-commerce industry beside that it has also created big challenges in this vein like fraud activities, vulnerable websites for online shopping, low quality product, delays in delivery, complex payment method and security issue (T. Ahmed, 2024). Online shopping, whereas particularly having lower carbon footprint compare to the traditional shopping, is influenced by various factors, such as consumer behavior, transportation, packaging and online transaction (Shafi et al., 2024a).

Regarding the online shopping, application safety must be given priority because payment gateway and personal details are shared and also the application must be user-friendly oriented with that top most privacy requires to be maintained (Al-Jahwari et al., 2018). Online shopping market is growing so it is crucial to find out the customer satisfaction which is related with safety, trust and quality of product (Moon et al., 2021). The majority of online buyers who are college student have positive impression of online shopping, some of them are concern about the safety while purchasing over the internet (Dr. Nair et al., 2023).

As established by (Monoarfa et al., 2024) for increasing the transparency of study in systematic literature reviews PRISMA model were employed so that the reliability and accuracy was created as a evidence. Recent study outlined by (Efendioğlu, 2024) suggest that this report writing for systematic review and meta-analysis (PRISMA) standard was also considered for systematic screening. Systematic review (PRISMA) was adopted for this study was an attempt to address the issue of online shopping (Shafi et al., 2024)

Online shopping safety concerns began to emerge in the mid-to-late 1990s, coinciding with the rise of e-commerce. As the internet became more widely accessible, online retail platforms such as Amazon and eBay started gaining popularity. The increase in online transactions highlighted the need for secure payment systems, data protection, and fraud prevention measures. Over time, these concerns grew more complex and comprehensive, leading to the development of various technologies and regulatory frameworks aimed at enhancing online shopping safety.

## **RESEARCH OBJECTIVE**

The major goal of the study was to understand the online shopping safety through a systematic literature review.

- a. Analyze the research trend of online shopping safety during 2020-2024.
- b. Analyze the research gap of online shopping safety.
- c. Discuss the future research according to the study.

## **RESEARCH QUESTION**

RQ1: What are the current trends of online shopping safety in a developing nation?

RQ2: What is the literature gap of online shopping safety?

RQ3: What suggestions are made for the future research through a systematic literature review?

## **METHODOLOGY**

A group of international researchers developed a framework named PRISMA in 2009 as a part of reporting item for systematic literature review (Monoarfa et al., 2024). PRISMA is a diagram containing four stages: identification, screening, eligibility and include. The PRISMA procedures were introduced for increasing the authentication and helping of research in systematic reviews. The PRISMA flow diagram, in generally, turned into a most uses instrument for presenting the information throughout the systematic review. This systematic review rejects many datasets because SLR aim to find the actual information that are genuinely related on the study.

### **Identification Stage**

In the first stage, Database was used to search the article employing Boolean operation “OR” and “AND” to narrow down the search result. The search keyword contained “online shopping safety” “online purchase intention” “online shopping risk” and “e-commerce experience”, along with the Boolean operation was employed to find the exact search queries. Furthermore, the researcher used a time frame from 2020 to 2024 to find out the current scenario of online shopping safety and anticipating future direction in this field.

### **Screening Stage**

Moving to the second stage, the screening process considered precisely identifying article by eliminating duplicate articles, others language article and which are not match with the study’s purpose. During the screening phase 40 documents were excluded and a total of 100 articles were considered relevant based on their title, abstract and connecting with the study. Mendeley reference manager was employed to conduct this stage with the exact focus on the title, abstract of content and related topic to the online shopping safety.

### **Eligibility Stage**

Following to the systematic literature review of multiple abstracts, researcher went to the third stage to address the second and third research objectives. During this stage document selection is dependent upon eligibility criteria. In the third stage 21 articles were excluded, while 79 were deemed eligible. Eligibility depends on the journal’s standard and accessibility of articles so that practitioner can read the full text articles.

### **Include Stage**

Moving to the last stage, out of the 79 full text articles, 61 articles were selected manually which were comprehensively alignment with the research topics. Finally, selected articles were used to forthcoming literature review.

Trust, social factor and technology adaption are influenced consumer to purchase product from online market place (Soeyatno et al., 2024). Even though e-commerce business has increased around the globe for past few years but several factors like faith, protection, and technology adaption has influence the customer to buy online product (Wahab et al., 2023). Financial risk, information risk and privacy risk have a significant influence on online purchase decision (Alrawad et al., 2023). Cognitive trust is influenced by the security and reputation whereas perceived risk is negatively effect on purchase intention of online shopping (Tran & Nguyen, 2022).

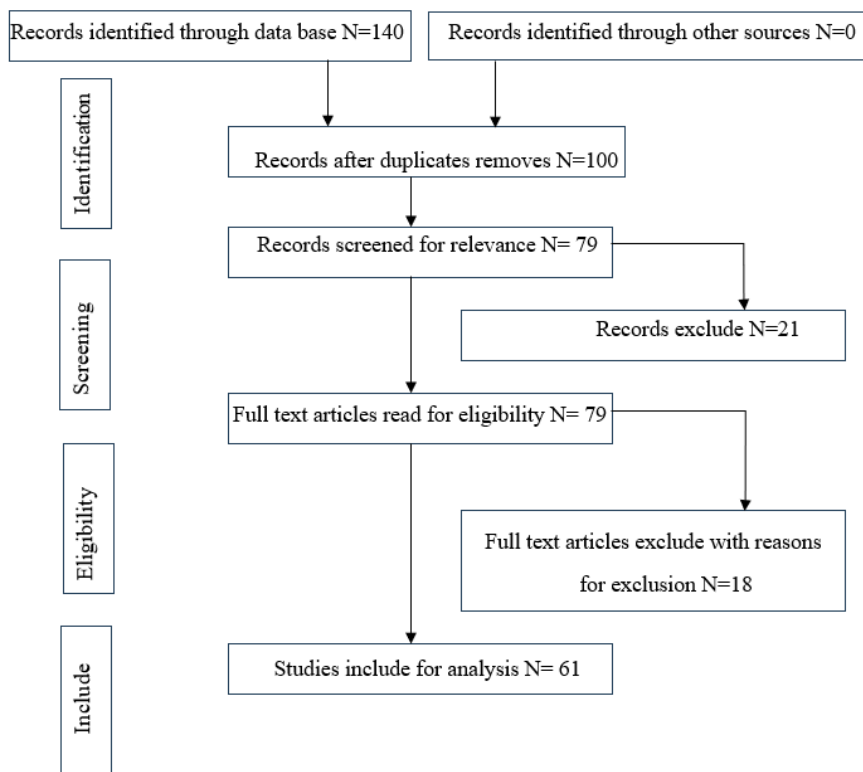


Table 1: List Of Selected Articles

SL	Title & Author
1	Purchasing Vegetables In The Digital Era: A Systematic Literature Review On Online Buying Behavior In E-Commerce (Soeyatno et al., 2024)
2	Customer Attitudes Towards Online Shopping: A Systematic Review Of The Influencing Factors (Abu-Alsondos et al., 2023)
3	Technology Acceptance Model To Factors Customer Switching On Online Shopping Technology: Literature Review (Setyoadi & Rahmawati, 2024)
4	Exploring Online Shopping Behavior In Dhaka, Bangladesh (Enam et al., 2024)
5	Uncover The Trends, Gaps, And Main Topics On Online Grocery Shopping: Bibliometric Analysis (Monoarfa et al., 2024)
6	Digital Consumer Behavior: A Systematic Literature Review (EFENDIOĞLU, 2024)
7	The Role Of Digitalization In Business And Management: A Systematic Literature Review (Calderon-Monge & Ribeiro-Soriano, 2024)
8	Factors Influencing Consumers' Attitude Towards Online Shopping In Rangpur City (Mridha et al., 2023)
9	E-Commerce In Bangladesh: Exploring The Challenges And Prospects Of Online Shopping Amid The Pandemic (T. Ahmed, 2024)
10	Customer Attitude, Buying Behavior And Satisfaction Towards Online Shopping: An Empirical Study In Some Selected Areas Of Bangladesh (Sen et al., 2024)
11	Demographic Analysis Of Online Grocery Shopping During The COVID-19 Pandemic: A Theoretical Perspective With An Expanded Technology Acceptance

SL	Title & Author
	Model (AbdulHussein et al., 2024)
12	Environmental Consciousness In The Digital Era Of Online Shopping: A Systematic And Bibliometric Review (Shafi et al., 2024b)
13	Meta-Analytic Review Of Online Purchase Intention: Conceptualising The Study Variables (Ghosh, 2024)
14	An Investigation Of cyber Attack Impact On Consumers' Intention To Purchase Online (Wahab et al., 2023)
15	Assessing Customers Perception Of Online Shopping Risks: A Structural Equation Modeling–Based Multigroup Analysis (Alrawad et al., 2023)
16	The Impact Of Security, Individuality, Reputation, And Consumer Attitudes On Purchase Intention Of Online Shopping: The Evidence In Vietnam (Tran & Nguyen, 2022)
17	Customer Attitudes Towards Online Shopping: A Systematic Review Of The Influencing Factors (Abu-Alsondos et al., 2023)
18	Online Grocery Shopping Intentions In The Post COVID-19 Context: A Case Of Millennial Generations In Bangladesh (Mondal & Hasan, 2023)
19	Online Shopping And Customer Satisfaction In College–Level Students In Kathmandu Valley (Manandhar & Timilsina, 2023)
20	A Systematic Literature Review Of Online Shopping In Sports Goods And Services: Considering The Role Of Trust And Perceived Risk (Dehghanpouri, 2021)
21	An Attempt To Find Out Loopholes In Online Shopping From The Prospective Of Women Customers And To Draw Suggestions (Singh, 2022)
22	Factors Affecting Online Shopping Behavior In Bangladesh: A Demographic Perspective (Hossain et al., 2022)
23	Growth And Trustworthiness Of Online Shopping & Business During The Pandemic: A Case Study On Bangladesh (Hasan et al., 2022)
24	Impact Of Hedonic Motivation, Utilitarian Motivation And Safety On Customer Loyalty In Online Shopping (Linge et al., 2022)
25	Online Grocery Shopping Behavior During COVID-19 Pandemic: An Interdisciplinary Explanation (Rout et al., 2022)
26	Online Retailers' Ethics And Its Effect On Repurchase Intention: The Mediating Role Of Perceived Risk (Yuniarti et al., 2022)
27	Online Shopping: A Survey On Consumer Buying Behavior In Bangladesh (S. Ahmed et al., 2022)
28	Perceived Benefits Of 'Online Shopping, Trust, And Safety' & Relationship With Purchase Intension: Women Customers Perspective (Singh & Bhatia, 2022)
29	Online Shopping: A Survey On Consumer Buying Behavior In Bangladesh (S. Ahmed et al., 2022)
30	Customer Satisfaction Towards Online Shopping (Abdallah, 2021)
31	Determinants Of Intention To Continue Usage Of (Al-Hattami, 2021) Online Shopping Under A Pandemic: COVID-19 (Al-Hattami, 2021)
32	Research On Consumer Attitude Toward Online Shopping: An Evidence From Bangladesh (Md. Rashedul Hasan & Affiliation: Master's Student, 2021)
33	The Impact Of Online Shopping Attributes On Customer Satisfaction And Loyalty: Moderating Effects Of E-Commerce Experience (Mofokeng, 2021)
34	Analysis Of Online Shoppers' Wish List And The Emergence Of Psychological Safety As A Salient Factor In Online Shopping Intentions (Kakar, 2020)
35	An Advanced Intelligence System In Customer Online Shopping Behavior And

SL	Title & Author
	Satisfaction Analysis (Moon et al., 2021)
36	Exploring Key Factors For Customer Satisfaction In Online Shopping: A Systematic Literature Review (Deyalage & Kulathunga, 2020)
37	To Bu(Y) Or Not To Bu(Y): Perceived Risk Barriers To Online Shopping Among South African Generation Y Consumers (Pentz et al., 2020)
38	Experiences and perceptions of cybercrime victims in Ghana: The Perspective of digital consumers of agricultural produce. (Mensah et al., 2023)
39	Enhancing trust in online grocery shopping through generative AI chatbots (Chakraborty et al., 2024)
40	E-Commerce: Issues, Opportunities, Challenges, and Trends (Santos et al., 2022)
41	The impact of perceived security on consumer trust in online shopping Kesharwani, A., & Bisht, S. S. (2021).
42	An investigation of cyber attack impact on consumers' intention to purchase online (Wahab et al., 2023).
43	Reimagining Marketing In The New Normal (Arora et al., 2020).
44	How Demographic Variables Impact Online Consumer Behavior Towards Online Shopping: The Case Of Yemen (Murshed, 2023).
45	Bridging the gap in cybersecurity awareness for online consumers: Insights and solutions (Singh & Gupta, M, 2023).
46	Emerging cyber threats in e-commerce: AI and deepfake challenges. Computers & Security (Wang et al., 2023).
47	AI-powered phishing: An evolving threat to e-commerce security (Alam et al., 2023)
48	Deepfake technology in online fraud: Emerging risks and countermeasures (Chen & Xu, 2022).
49	Supply chain vulnerabilities in e-commerce: Addressing third-party risks (Novak & Taylor, 2023).
50	IoT and its implications for online shopping security (Patel et al., 2022).
51	Social media and its role in e-commerce scams: A comprehensive review (Liu & Zhang, 2023).
52	Security challenges in e-commerce for SMEs (Smith & Jones, 2022).
53	Cybersecurity training gaps in SMEs: A global perspective (Lee et al. 2022).
54	Regulatory challenges for SMEs in online shopping security (Patel et al. 2023).
55	Building trust in e-commerce for SMEs: The role of cybersecurity (Chen & Yu, 2023).
56	Online shopping safety in developing nations (Rahman et al., 2022).
57	Trust and security in e-commerce: Cultural perspectives from East and West (Tan & Tan, 2021).
58	The impact of technological infrastructure on online shopping security in developing

SL	Title & Author
	countries (Lee & Zhang, 2023).
59	Data privacy concerns in cross-cultural e-commerce (Kaur & Ranjan, 2023).
60	Risk perception in online shopping: A cultural approach (Choi & Park, 2022).
61	Cross-cultural differences in e-commerce trust and privacy concerns: A comparative study (Choi et al. 2023).

## ANALYSIS OF RESEARCH TRENDS: ONLINE SHOPPING SAFETY (2020-2024)

### Increased Awareness and Concern Among Consumers

Consumer awareness of online shopping safety has vastly increased (EFENDIOĞLU, 2024). A survey conducted this year found that 92% of American consumers now consider security an important factor when they make purchases online (Exploding Topics, 2024). The increasing suspicion of online information, new concerns about fake reviews and AI-generated errors, has led people to trust reputable platforms with their information and follow established brands because they believe these suppliers offer truth (Wall Street Journal, 2024).

### Fraud and Scams on the Rise

On-line frauds--and particularly phishing--are still problems (Mensah et al., 2023). 41.65% of all financial phishing targets last year were shopping platforms (InBeat Agency, 2024). In addition, with shopping peaks bringing fake websites again, leaving police agencies such as the FBI reminding us to double-check the identity of those sites before making any transactions, we are faced with another serious problem (The Sun, 2024).

### Retailers Responding to Security Needs

Retailers have recognized consumers' demands for shopping security (Sen et al., 2024). For example, 83% of consumers will feel more secure purchasing from brands with solid protections against fraud (Exploding Topics, 2024). Further, 94% of today's enterprises know that poor information security will deter potential customers (Forbes, 2024).

### Technical Developments and Threats on the Horizon

While technological advancements improve one's online shopping experience, we may also object new threats (Chakraborty et al., 2024). AI in cybercrime--including chatbots used for phishing as well as deepfakes--turned out to be a very pressing problem this year (Wikipedia, 2024).

Internet Safety Studies, 2020-2024: As both consumers and vendors have found in enhanced cap fraud, sanctions on user privacy and effective measures to regulate the net, these issues have all become more important since the close of last year. But the dynamic nature of internet threats calls for constant vigilance and adaptation.

### Research Gap in Online Shopping Safety

As e-commerce continues to surge, guaranteeing safe online shopping experiences has never been more important. Santos et al.( 2022) Studies show a considerable improvement in online payments, security, and customer education. Despite that, a number of research gaps remain.

### Consumer Awareness and Behaviour

On the one hand, consumer awareness and conduct is a key factor in online shopping security and will affect the success of protection measures. Despite improvements in

technology, creating robust frameworks for secure transactions, a significant gap is found regarding consumer perception and response towards online safety mechanisms (Kesharwani & Bisht, 2021).

### ***Insufficient Knowledge of Security Features***

Research shows that a huge percentage of online shoppers do not know any common security feature, including HTTPS, digital certificates, or two-factor authentication. The Sentence: For example: Wahab et al. (2021) reported that less than 40% of respondents correctly identified a safe website. Without this knowledge, consumers become sitting targets for cyberattacks.

### ***Trust and Risk Perception***

Consumers trust the e-commerce platform based on the brand rather than the technical security features of the site. This was illustrated by the work of Arora et al. (2020) who had technology savvy respondents still being overly confident in the branding brands with products targeted at less risk aware consumers. This kind of conduct has added to phishing and adding fraudulent destinations.

### ***Socio-Demographic Factors***

Demographic variables like age, educational level and level of experience on the use of Internet, significantly affect consumer awareness. We know that younger users are typically more aware than older users to some extent, but at the same time, they engage in riskier online behavior, such as ignoring privacy policies (Murshed, 2023). On the other hand, the older users hardly know the basic security procedures which make them prone to scam.

### ***Prior Gaps in Education on Security***

The scope of education is often generic (e.g., awareness campaign or flyer on safe online shopping) and does not account for consumer group heterogeneity. Despite these limitations, Singh and Gupta (2023) advocate for a customized, scenario specific training as a practical method that could significantly enhance consumer threat detection. Visual representation of the belief development cycle.

Closing these gaps will require action from multiple angles, such as user-focused security education, the communication of security and safety features, and the nurturing of a culture of safety in eCommerce settings.

### ***Emerging Threats in Online Shopping***

As e-commerce becomes more prevalent, new risks are also arising around it. New technologies create new dangers, as traditional threats — phishing, spyware — converge with a whole set of nightmarish circumstances. First, these emergent risks also show that current online safety systems and existing consumer habits lead to the ongoing situation under which vulnerabilities continue to exist in safety online shopping (Wang et al., 2023).

### ***Phishing Attacks Powered by AI***

Artificial intelligence (AI) may be used to construct phishing campaigns. While phishing has grown increasingly technical over time, AI technology-as demonstrated by the accuracy of digital impersonation far surpassing human capability-goes well beyond anything human beings can create. For instance, Alam et al. Researchers recently found that AI-generated phishing e-mails are 30% more successful than their traditional counterparts for customers.

### ***Deepfakes***

Deepfakes, artificially altering the audio and video of a person in a convincing way, are increasingly being deployed to commit fraud against e-commerce retailers. Cybercriminals use deepfakes to impersonate company personnel, customer service representatives or in

some cases even customers themselves and fraudulently access accounts or make illicit transactions (Chen & Xu, 2022).

### ***Supply Chain Attacks***

Despite the utilization of third-party suppliers for software, money processing and logistics by many e-commerce companies, a number also service threat actors with access so extensive it spreads across the entire supply chain. This does not necessarily mean an intrusion at major business level with cut-and-dried methods of operation. In a relative sense of hindsight, as identified by Novak and Taylor (2023), these small security flaws in third-party integrations result in vast data breaches.

### ***IoT Vulnerabilities***

Embedded with the online shopping ecosystem are the Internet of Things (IoT) (e.g. devices like smart home assistants that can order groceries), which bring new kinds of security risks with them. As Patel et al concluded, Lory et al indicated (2022), unsecured IoT devices are perfect beachheads for hackers from home wi-fi or public network: they provide an entry point into user data and financial information.

### ***Social media/Social engineering***

The line between e-commerce and social media is becoming increasingly blurred, which means that there are now higher risks for social engineering attacks. Swindlers making fake ads, shoddy merchandise and phoney deals use social media to target consumers all the time (Liu & Zhang, 2023).

Future research should then be directed to adaptive cyber security, better consumer detection and cooperative efforts among interested stakeholders such as technology providers, governments and consumers to deal with these threats.

### ***Small and Medium Enterprises (SMEs)***

Although large e-commerce platforms are usually in the spotlight during discussions about safe online shopping, small and medium enterprises (SMEs) have apparent security concerns of their own. Small and medium-sized enterprises (SMEs) are a major driving force of the global economy, but face challenges of inadequate resources as well as expert know-how to undertake concrete cybersecurity measures, making them highly susceptible to threats (Smith & Jones, 2022).

### ***Cybersecurity budgets are limited***

Due to the limited budgets SMEs operate on, this can also restrict their access to security technology. Consequently, they depend on basic, often antiquated, security measures and become open to cyber breaches. According to Alam et al. According to an open text survey - Cybersecurity In Your SMB.

### ***Lack of education and training***

Most SME owners & employees are not sufficiently trained to identify or respond to common cycle threats. The ignorance is what makes them easy prey to phishing, ransomware and data breaches. Research by Lee et al. As noted by Lallie Tzeng (2022), over 50% of SMEs do not offer cybersecurity training for their employees.

### ***Weaknesses in Services Provided by Third Parties***

Small and medium-sized enterprises (SMEs) typically outsource their payment, inventory, and other services to third-party providers. These dependencies introduce further security weaknesses because bad actors can target the weakest link in the supply chain (Novak & Taylor, 2023).

***Not Complying With Regulations***

But because SMEs often have limited resources and expertise, they often fail to cope with regulatory requirements in the fields of data protection and cybersecurity. Failure to comply only augments the exposure of data breaches but also puts SMEs at a heightened risk of legal and financial penalties (Patel et al., 2023).

***Challenges in Customer Trust***

SMEs lack the facility and trust associated with big e-commerce sites, and therefore have to work harder. According to (Chen & Yu, 2023), due to the high rate of data leaks and the nature of information technology companies, a single breach of security can seriously harm reputation and deter prospective buyers — and threaten long-term viability.

SMEs need cost-effective and scalable cybersecurity solutions to tackle these challenges. Targeted support should be provided by governments and industry associations through the provision of subsidies and training, as well as simplified regulatory frameworks. Also, partnerships with tech developers may enable SMEs to invest in sophisticated security solutions at less financial demand.

***Cross-Cultural Studies***

E-commerce is inherently global and thus warrants greater insight into cross-cultural determinants of online shopping safety perceptions and behaviors. Prior studies have tended to concentrate on developed countries whereas little is known about security perceptions of online shoppers belonging to different cultural backgrounds. These voids can be resolved through cross-cultural studies, which provide insights into any differences regarding attitude, trust and behavior towards online shopping safety (Rahman et al., 2022).

***Cultural Perceptions of Trust and Security***

Trust is a critical factor in online shopping, but cultural differences play a significant role in shaping how consumers evaluate security. For example, consumers in collectivist societies, such as many Asian countries, tend to place more trust in recommendations from social networks or family members, while consumers in individualistic cultures may prioritize technological security measures (Tan & Tan, 2021). These cultural nuances affect the level of trust shoppers place in security protocols and the likelihood of adopting them.

***Technological Infrastructure and Security Awareness***

The availability and adoption of security technologies vary widely across countries. In developed nations, where internet infrastructure is robust, users may have a higher level of cybersecurity awareness and access to advanced security tools. Conversely, in developing countries, limited technological resources and infrastructure may result in lower awareness and higher vulnerability to cyber threats (Rahman et al., 2022). For instance, a study by Lee and Zhang (2023) revealed that online shoppers in low-income countries are less likely to use secure payment methods like credit cards or two-factor authentication.

***Privacy Concerns and Data Protection***

Different cultures have varying attitudes toward privacy and data protection. Consumers in countries like the EU, with strong data protection laws like the GDPR, may be more conscious of their privacy rights and prefer platforms that ensure robust data security. In contrast, consumers in countries with weaker data protection laws may be less concerned about privacy issues, leading to increased exposure to online risks (Kaur & Ranjan, 2023).

***Consumer Behavior and Risk Perception***

Cultural differences also influence how individuals perceive risks associated with online shopping. For example, consumers from high-risk-averse cultures may be more hesitant to engage in online shopping unless there is clear evidence of security measures in place. On

the other hand, consumers from cultures with lower risk aversion may be more willing to engage in online transactions without fully understanding the potential security risks (Choi & Park, 2022).

### **Regional Regulatory Variations**

Regional differences in regulations further complicate the landscape of online shopping safety. While some countries have strict regulations regarding e-commerce security, others may have minimal or inconsistent enforcement of cybersecurity laws. This regulatory inconsistency can lead to disparities in online shopping safety, with consumers in less regulated regions facing greater risks (Choi et al., 2023).

### **Recommendations**

Future research should prioritize cross-cultural studies to develop globally applicable online shopping security strategies. This includes understanding regional attitudes toward trust, privacy, and security, as well as adapting educational efforts to suit cultural contexts. Moreover, collaborations between global e-commerce platforms and local regulators could enhance security measures in regions with weaker cybersecurity infrastructures.

### **Future Research Directions in Online Shopping Safety Based on Previous Studies**

Drawing from the previous discussions on consumer awareness, emerging threats, SMEs, and cross-cultural studies, several promising avenues for future research in online shopping safety can be identified. These directions are aimed at addressing the existing gaps in the literature and improving the security and overall online shopping experience. Below are key areas that require further exploration:

#### ***1. Enhancing Consumer Awareness and Behavior***

Given that consumer awareness is a significant factor in online shopping safety, future research should focus on the following areas:

##### ***Personalized Awareness Programs***

Research should explore how educational campaigns can be customized to target specific demographic groups (e.g., age, education level, and cultural background). For instance, Chatterjee et al. (2022) emphasized the need for scenario-based training, which can be expanded upon to develop more effective awareness programs that are personalized to the individual's level of knowledge and behavioral patterns.

**Behavioral Interventions:** Future studies should examine the psychological factors that drive risky behavior in online shopping, such as the role of trust and overconfidence in e-commerce platforms. Exploring the effectiveness of behavioral nudges and interventions could help reduce risky online shopping behaviors (Yadav & Mahara, 2022).

**Longitudinal Studies on Awareness Impact:** A longitudinal approach could be adopted to assess the long-term effectiveness of security education campaigns in enhancing consumer awareness and their ability to recognize and avoid online threats.

#### ***2. Addressing Emerging Threats in E-Commerce***

With the rise of sophisticated threats like AI-driven phishing attacks, deepfakes, and IoT vulnerabilities, future research must:

**AI-Driven Cybersecurity Solutions:** Researchers should focus on the development of advanced AI-based solutions to detect and mitigate cyber threats, particularly in detecting AI-generated phishing attempts and deepfake scams. Investigating the efficacy of machine learning and AI algorithms in real-time threat detection can enhance security measures (Wang et al., 2023).

**IoT Security in E-Commerce:** As more devices become interconnected, research should focus on securing IoT in the e-commerce ecosystem. Exploring secure design principles for IoT devices and evaluating their role in the security framework for online shopping can help mitigate vulnerabilities (Patel et al., 2022).

**Psychological and Social Engineering Attacks:** Further exploration is needed into how social engineering tactics, particularly through social media, influence online shoppers. Research could focus on understanding how scammers exploit human psychology through targeted social media advertisements and fake reviews (Liu & Zhang, 2023).

### ***3. SMEs and Online Shopping Security***

**As SMEs face distinct challenges in adopting cybersecurity measures, future studies could:**  
**Affordable Security Solutions for SMEs:** Research could explore the development of low-cost, scalable security tools tailored for SMEs, focusing on enhancing their capacity to secure online transactions without incurring significant financial burdens. This could include open-source security frameworks or low-cost cybersecurity services specifically designed for smaller enterprises (Smith & Jones, 2022).

**Risk Management Strategies for SMEs:** There is a need to investigate how SMEs perceive and manage cybersecurity risks. Future research could identify best practices for risk management and offer practical guidelines that SMEs can implement to reduce vulnerabilities, considering the limitations in resources and expertise.

**Cybersecurity Collaboration Networks:** Further research could explore the potential of collaborative networks between SMEs, technology providers, and government agencies to share cybersecurity resources, information, and training.

### ***4. Cross-Cultural Studies in Online Shopping Safety***

Cross-cultural differences in online shopping behavior and security awareness present significant research opportunities:

**Cross-Cultural Security Awareness Campaigns:** Research should focus on designing culturally sensitive online shopping safety campaigns. These campaigns would be based on varying levels of trust, privacy concerns, and technological adoption, especially in emerging markets with distinct cultural attitudes toward online transactions (Rahman et al., 2022).

**Understanding Privacy Concerns Across Cultures:** Further research is needed to examine how different cultures view privacy and how these views influence online shopping behaviors. Comparative studies on privacy concerns in developed and developing nations could reveal how cultural attitudes affect the adoption of security features, such as encryption or two-factor authentication (Kaur & Ranjan, 2023).

**Global E-Commerce Security Standards:** As global e-commerce continues to grow, there is a need for research on creating universal security standards that can address cross-cultural challenges while maintaining high levels of privacy and trust. This research could explore how regional regulatory frameworks interact with international standards and whether harmonization is possible (Choi et al., 2023).

The future of online shopping safety research lies in a multifaceted approach that addresses both technological advancements and human factors. As e-commerce evolves, it is essential to focus on developing adaptive and culturally sensitive security solutions, increasing consumer awareness, and understanding the unique challenges faced by SMEs and diverse global populations. A holistic approach that combines education, technological innovation, and cross-cultural understanding will be key to improving online shopping safety in the coming years.

## CONCLUSION

The current systematic literature review brings attention on perceptions of online shopping safety in developing nations during the period of 2020–2024. The results show that, even though online shopping has become a crucial part of a consumer's habits, it brings along headwinds such as unreliable websites, security issues, receipt of low quality products, and delayed delivery. Yet, additional development of digital and technological infrastructure alongside increased U-Apop client focused business models offer signs to formal policy innovation in the high-value e-commerce market.

It emphasizes the need for consumer trust with adopting technologies, and digital literacy while shopping online to create a safe and trustworthy online shopping environment. Using the PRISMA framework, through the identification of major trends, gaps and future directions, this review highlights a lack of regulation and cooperation between stakeholders.

The study offers actionable insight on how to alleviate online shopping safety concerns for policymakers, businesses, and researchers alike. The government can take a grave initiative in building proper digital mechanism, enforce stiff regulations and conduct awareness programmes to help consumers distance from any online dangers and follow the right practice. While businesses should focus on transparency, security, and customer satisfaction to gain trust and loyalty for the long term.

In summary, though there has been considerable advancement in the literature addressing online shopping safety, future investigations should include new approaches to close the gap between what consumers want and what is currently available. From a holistic approach, by eliminating the mentioned challenges developing countries would be able to use the greater potential of e-commerce ensuring safety and efficiency of consumer shopping basket world wide.

## REFERENCE

- Abdallah, N. (2021). Customer Satisfaction towards Online Shopping. *International Journal of Current Science Research and Review*, 04(07). <https://doi.org/10.47191/ijcsrr/v4-i7-11>
- AbdulHussein, A., Dimitrov, S., & Cozzarin, B. (2024). Demographic analysis of online grocery shopping during the COVID-19 pandemic: a theoretical perspective with an expanded technology acceptance model. *Cogent Business and Management*, 11(1). <https://doi.org/10.1080/23311975.2024.2336712>
- Abu-Alsondos, I. A., Alkhawaldi, A. F., Salhab, H. A., Shehadeh, M., & Ali, B. J. A. (2023). Customer attitudes towards online shopping: A systematic review of the influencing factors. *International Journal of Data and Network Science*, 7(1), 513–524. <https://doi.org/10.5267/j.ijdns.2022.12.013>
- Ahmed, S., Munir, M. S., & Islam, T. (2022). Online Shopping: A Survey on Consumer Buying Behavior in Bangladesh. *European Scientific Journal, ESJ*, 18(15), 93. <https://doi.org/10.19044/esj.2022.v18n15p93>
- Ahmed, T. (2024). *E-commerce in Bangladesh : Exploring the Challenges and Prospects of Online Shopping amid the Pandemic*. June. <https://doi.org/10.5281/zenodo.11519513>
- Alam, S., Chen, Y., & Wang, J. (2023). AI-powered phishing: An evolving threat to e-commerce security. *Cybersecurity Journal*, 28(2), 143–156.
- Alam, S., Gupta, R., & Reddy, P. (2023). Budget constraints in SME cybersecurity: Implications and strategies. *Journal of Cybersecurity Research*, 18(2), 112–128.
- Al-Hattami, H. M. (2021). Determinants of intention to continue usage of online shopping

- under a pandemic: COVID-19. *Cogent Business and Management*, 8(1). <https://doi.org/10.1080/23311975.2021.1936368>
- Al-Jahwari, N. S., Khan, M. F. R., Al Kalbani, G. K., & Al Khansouri, S. S. (2018). Factors influencing customer satisfaction of online shopping in Oman – Youth perspective. *Humanities and Social Sciences Reviews*, 6(2), 64–73. <https://doi.org/10.18510/hssr.2018.628>
- Alrawad, M., Lutfi, A., Alyatama, S., Al Khattab, A., Alsoboa, S. S., Almaiah, M. A., Ramadan, M. H., Arafa, H. M., Ahmed, N. A., Alsyoud, A., & Al-Khasawneh, A. L. (2023). Assessing customers perception of online shopping risks: A structural equation modeling–based multigroup analysis. *Journal of Retailing and Consumer Services*, 71(October 2022). <https://doi.org/10.1016/j.jretconser.2022.103188>
- Alshurideh, M. T., Bataineh, A. Q., & Emeagwali, O. L. (2021). Consumer behavior and cybersecurity awareness in e-commerce: A cross-sectional study. *Journal of Electronic Commerce Research*, 22(3), 134–147.
- Arora, A., Dahlstrom, P., Hazan, E., Khan, H., & Khanna, R. (2020). Reimagining marketing in the next normal. In *McKinsey & Company* (Issue July). <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/reimagining-marketing-in-the-next-normal>
- Calderon-Monge, E., & Ribeiro-Soriano, D. (2024). The role of digitalization in business and management: a systematic literature review. In *Review of Managerial Science* (Vol. 18, Issue 2). Springer Berlin Heidelberg. <https://doi.org/10.1007/s11846-023-00647-8>
- Chakraborty, D., Kumar Kar, A., Patre, S., & Gupta, S. (2024). Enhancing trust in online grocery shopping through generative AI chatbots. *Journal of Business Research*, 180(December 2023), 114737. <https://doi.org/10.1016/j.jbusres.2024.114737>
- Chatterjee, S., Bhowmick, S., & Das, T. (2022). Socio-demographic impacts on online security awareness. *International Journal of Cyber Behavior, Psychology and Learning*, 12(2), 89–101.
- Chen, M., & Xu, H. (2022). Deepfake technology in online fraud: Emerging risks and countermeasures. *Journal of Digital Crime Studies*, 15(1), 45–61.
- Chen, Y., & Yu, L. (2023). Building trust in e-commerce for SMEs: The role of cybersecurity. *Journal of Digital Commerce*, 14(1), 89–102.
- Choi, S., & Park, M. (2022). Risk perception in online shopping: A cultural approach. *International Journal of E-Commerce Studies*, 17(4), 78–92.
- Choi, S., Lee, J., & Kang, D. (2023). Cross-cultural differences in e-commerce trust and privacy concerns: A comparative study. *Journal of International Business Studies*, 52(2), 320–338.
- Dehghanpouri, H. (2021). A Systematic Literature Review of Online Shopping in Sports Goods and Services: Considering the Role of Trust and Perceived Risk. *Research in Sport Management and Marketing*, March. [http://journal.uma.ac.ir/article\\_1317\\_2ed24bc7bc495fc19b5622aaec70f8d8.pdf](http://journal.uma.ac.ir/article_1317_2ed24bc7bc495fc19b5622aaec70f8d8.pdf)
- Deyalage, P. A., & Kulathunga, D. (2020). Exploring Key Factors for Customer Satisfaction in Online Shopping: A Systematic Literature Review. *University of Sri Jayewardenepura (VJM)*, 06(1), 163–190. <http://www.dr.lib.sjp.ac.lk/handle/123456789/10474>
- Dr. Nair, R. K., Dr. Rajni Mathur, N., Dr. Lavanya, D., Yadav, N., Dr. Banerjee, D., & Akilesh, S. (2023). Service Quality and Customer Satisfaction towards Online Shopping- A Theoretical Framework. *Eur. Chem. Bull*, 5, 622–633.

- <https://doi.org/10.13140/RG.2.2.13777.34400>
- E-Cab. (2024). *E-commerce Association of Bangladesh*.
- Efendioğlu, İ. H. (2024). *DIGITAL CONSUMER BEHAVIOR: A SYSTEMATIC LITERATURE REVIEW DIGITAL CONSUMER BEHAVIOR: A SYSTEMATIC*. May. <https://doi.org/10.32936/pssj.v8i1.479>
- EFENDIOĞLU, İ. H. (2024). Digital Consumer Behavior: a Systematic Literature Review. *Prizren Social Science Journal*, 8(1). <https://doi.org/10.32936/pssj.v8i1.479>
- Enam, A., Azad, I. I., & Afrin, S. (2024). Exploring online shopping behavior in Dhaka, Bangladesh. *Transportation Research Interdisciplinary Perspectives*, 25(March 2024), 101081. <https://doi.org/10.1016/j.trip.2024.101081>
- Exploding Topics. (2024). Online shopping statistics. Retrieved from <https://explodingtopics.com/blog/online-shopping-stats>
- Forbes. (2024). Top retail and e-commerce trends. Retrieved from <https://www.forbes.com/councils/forbesbusinesscouncil/2024/06/25/retail-and-e-commerce-in-2024-top-trends-to-watch/>
- Ghosh, M. (2024). Meta-analytic review of online purchase intention: conceptualising the study variables. *Cogent Business and Management*, 11(1). <https://doi.org/10.1080/23311975.2023.2296686>
- Hasan, M., Bijoy, I., Rubi, M. A., Chowdury, S., & Rahman, S. (2022). Growth and Trustworthiness of Online Shopping & Business during the Pandemic: A Case Study on Bangladesh. *Journal of Sales, Service and Marketing Research*, 1. [www.matjournals.com](http://www.matjournals.com)
- Hossain, M. K., & Jawad, S. S. (2022). *Factors affecting online shopping behavior in Bangladesh: A demographic perspective Business Ecosystem & Strategy Factors affecting online shopping behavior in Bangladesh: A demographic perspective*. June. <https://doi.org/10.36096/ijbes.v4i3.351>
- Hossain, M. K., Md Abdus Salam, & Sheikh Sakib Jawad. (2022). Factors affecting online shopping behavior in Bangladesh: A demographic perspective. *International Journal of Business Ecosystem & Strategy* (2687-2293), 4(3), 13–22. <https://doi.org/10.36096/ijbes.v4i3.351>
- InBeat Agency. (2024). Online shopping statistics. Retrieved from <https://inbeat.agency/blog/online-shopping-statistics>
- Kakar, A. (2020). *Analysis of Online Shoppers' Wish List and the emergence of Psychological Safety as a Salient Factor in Online Shopping Intentions*. January, 1022–1031.
- Kaur, H., & Ranjan, R. (2023). Data privacy concerns in cross-cultural e-commerce. *Journal of Cybersecurity & Digital Privacy*, 8(1), 40–56.
- Kesharwani, A., & Bisht, S. S. (2021). The impact of perceived security on consumer trust in online shopping. *International Journal of Consumer Studies*, 45(1), 76–89.
- Lee, J., & Zhang, L. (2023). The impact of technological infrastructure on online shopping security in developing countries. *Journal of Global E-Commerce*, 14(3), 213–228.
- Lee, J., Park, S., & Kim, H. (2022). Cybersecurity training gaps in SMEs: A global perspective. *Small Business Cybersecurity Review*, 7(3), 55–70.
- Linge, A., Sanjeev, S., Kakde, B., & Singh, M. (2022). Impact of Hedonic Motivation, Utilitarian Motivation and Safety on Customer Loyalty in Online Shopping. *International Research Journal of Management Science & Technology*, 13(10), 96–107. <http://www.irjmst.com>

- Liu, X., & Zhang, W. (2023). Social media and its role in e-commerce scams: A comprehensive review. *Journal of Social Media Studies*, 11(3), 210–226.
- Manandhar, R. B., & Timilsina, J. (2023). Online Shopping and Customer Satisfaction in College–Level Students in Kathmandu Valley. *Journal of Business and Management*, 7(02), 76–88. <https://doi.org/10.3126/jbm.v7i02.62588>
- Md. Rashedul Hasan, A. S. N., & Affiliation: Master's Student, B. S. (2021). *Research on consumer attitude toward online shopping An evidence from Bangladesh.pdf*. May, 161–170. <https://doi.org/http://www.doi-ds.org/doi/10.21203.2021.98269899/UIJIR>
- Mensah, R. O., Mensah, P., & Opoku, D. (2023). Experiences and perceptions of cybercrime victims in Ghana: The Perspective of digital consumers of agricultural produce. *Cogent Education*, 10(2). <https://doi.org/10.1080/2331186X.2023.2285623>
- Mofokeng, T. E. (2021). The impact of online shopping attributes on customer satisfaction and loyalty: Moderating effects of e-commerce experience. *Cogent Business and Management*, 8(1). <https://doi.org/10.1080/23311975.2021.1968206>
- Mondal, S., & Hasan, A. A.-T. (2023). Online grocery shopping intentions in the post COVID-19 context: a case of millennial generations in Bangladesh. *South Asian Journal of Marketing*, October. <https://doi.org/10.1108/sajm-01-2023-0001>
- Monoarfa, T. A., Sumarwan, U., Suroso, A. I., & Wulandari, R. (2024). Uncover the trends, gaps, and main topics on online grocery shopping: Bibliometric analysis. *Heliyon*, 10(4), e25857. <https://doi.org/10.1016/j.heliyon.2024.e25857>
- Moon, N. N., Talha, I. M., & Salehin, I. (2021). An advanced intelligence system in customer online shopping behavior and satisfaction analysis. *Current Research in Behavioral Sciences*, 2(August), 100051. <https://doi.org/10.1016/j.crbeha.2021.100051>
- Mridha, M. M., Hossain, M. S., Chowdhury, M. S., Al-Imran, M., & Debnath, D. (2023). Factors influencing consumers' attitude towards online shopping in Rangpur City. *International Multidisciplinary Research Journal*, May, 15–24. <https://doi.org/10.25081/imrj.2023.v13.8324>
- Murshed, N. A. (2023). How Demographic Variables Impact Online Consumer Behavior Towards Online Shopping: the Case of Yemen. *The Journal of Academic Social Sciences*, 147(147), 241–256. <https://doi.org/10.29228/asos.73198>
- Nguyen, T. T. H. (2024). Assessing Risk Factors Affecting Customers' Online Shopping. *IRJEMS International Research Journal of Economics and Management Studies*, 3(4), 125–129. <https://doi.org/10.56472/25835238/IRJEMS-V3I4P118>
- Novak, T., & Taylor, A. (2023). Supply chain vulnerabilities in e-commerce: Addressing third-party risks. *Journal of Cybersecurity Research*, 20(4), 302–318.
- Patel, R., Sharma, D., & Kumar, A. (2022). IoT and its implications for online shopping security. *International Journal of Digital Commerce*, 9(3), 67–82.
- Patel, R., Sharma, D., & Kumar, A. (2023). Regulatory challenges for SMEs in online shopping security. *International Journal of Digital Commerce*, 10(2), 67–81.
- Pentz, C. D., du Preez, R., & Swiegers, L. (2020). To bu(Y) or not to bu(Y): Perceived risk barriers to online shopping among South African generation Y consumers. *Cogent Business and Management*, 7(1). <https://doi.org/10.1080/23311975.2020.1827813>
- PMC. (2022). Changes in shopping behavior post-COVID-19. Retrieved from <https://pmc.ncbi.nlm.nih.gov/articles/PMC9414037/>
- Rahman, T., Khan, M. R., & Alam, S. (2022). Online shopping safety in developing nations: A case study of Bangladesh. *Journal of Cybersecurity*, 18(4), 301–320.
- Report Business Star. (2023). Central complaint management system to prevent e-commerce

- fraud. *The Daily Star*.
- Rout, K., Sahoo, P. R., Bhuyan, A., Tripathy, A., & Smrutirekha. (2022). Online grocery shopping behavior during COVID-19 pandemic: An interdisciplinary explanation. *Cogent Business and Management*, 9(1). <https://doi.org/10.1080/23311975.2022.2084969>
- Santos, V., Augusto, T., Vieira, J., Bacalhau, L., Sousa, B., & Pontes, D. (2022). E-commerce: Issues, opportunities, challenges, and trends. *Promoting Organizational Performance Through 5G and Agile Marketing*, March 2024, 224–244. <https://doi.org/10.4018/978-1-6684-5523-4.ch012>
- Seddique Ul Huque Sazzad. (2023, January). F-commerce is the new shopping mall. *Dhaka Tribune*.
- Sen, T., Khatun, M., Khan, M. A., & Rahman, M. A. (2024). Customer attitude, buying behavior and satisfaction towards online shopping: An empirical study in some selected areas of Bangladesh. *Archives of Agriculture and Environmental Science*, 9(1), 76–84. <https://doi.org/10.26832/24566632.2024.0901012>
- Setyoadi, E. T., & Rahmawati, T. (2024). Technology Acceptance Model to Factors Customer Switching on Online Shopping Technology: Literature Review. *Sinkron*, 9(1), 196–209. <https://doi.org/10.33395/sinkron.v9i1.12993>
- Shafi, S., Mohamed, W. N., Damaianti, I., & Salleh, H. S. (2024a). *Environmental Consciousness in the Digital Era of Online Shopping : A Systematic and Bibliometric Review* *Environmental Consciousness in the Digital Era of Online Shopping : A Systematic and Bibliometric Review*. June. <https://doi.org/10.18280/ij dne.190327>
- Shafi, S., Mohamed, W. N., Damaianti, I., & Salleh, H. S. (2024b). Environmental Consciousness in the Digital Era of Online Shopping: A Systematic and Bibliometric Review. *International Journal of Design and Nature and Ecodynamics*, 19(3), 971–984. <https://doi.org/10.18280/ij dne.190327>
- Singh, N. (2022). *An attempt to find out loopholes in online shopping An attempt to find out loopholes in online shopping from the prospective of women customers and to draw suggestions*. January.
- Singh, N., & Bhatia, A. (2022). *Perceived Benefits of “Online Shopping, Trust, and Safety” & Relationship with Purchase Intension: Women Customers perspective*. December. [www.forbes.com](http://www.forbes.com)
- Singh, R., & Gupta, M. (2023). Bridging the gap in cybersecurity awareness for online consumers: Insights and solutions. *Journal of Digital Safety and Privacy*, 6(1), 43–57.
- Smith, A., & Jones, P. (2022). Security challenges in e-commerce for SMEs. *Journal of Business Research*, 56(3), 212–220.
- Soeyatno, R. F., Darjanto, A., Syaukat, Y., & Nurmalina, R. (2024). Purchasing Vegetables in the Digital Era: A Systematic Literature Review on Online Buying Behavior in E-Commerce. *Agro Bali : Agricultural Journal*, 6(3), 524–542. <https://doi.org/10.37637/ab.v6i3.1492>
- Tan, S. F., & Tan, S. C. (2021). Trust and security in e-commerce: Cultural perspectives from East and West. *Asian Journal of Business Research*, 15(2), 93–104.
- The Sun. (2024). FBI warns Chrome & Safari users about scams. Retrieved from <https://www.the-sun.com/tech/12994991/fbi-chrome-safari-holiday-sales-scams/>
- Tran, V. D., & Nguyen, T. D. (2022). The impact of security, individuality, reputation, and consumer attitudes on purchase intention of online shopping: The evidence in Vietnam. *Cogent Psychology*, 9(1). <https://doi.org/10.1080/23311908.2022.2035530>
- Wahab, F., Khan, I., Kamontip, Hussain, T., & Amir, A. (2023). An investigation of cyber

- attack impact on consumers' intention to purchase online. *Decision Analytics Journal*, 8(August), 100297. <https://doi.org/10.1016/j.dajour.2023.100297>
- Wall Street Journal. (2024). Five consumer trends for 2025. Retrieved from <https://www.wsj.com/articles/eating-in-designer-stores-shopping-on-tiktok-five-consumer-trends-for-2025-7af3cc02>
- Wang, Y., Chen, L., & Lee, H. (2023). Emerging cyber threats in e-commerce: AI and deepfake challenges. *Computers & Security*, 113, 102579.
- Wikipedia. (2024). Cybercrime. Retrieved from <https://en.wikipedia.org/wiki/Cybercrim>
- Yadav, K., & Mahara, S. (2022). Trust, risk perception, and consumer behavior in e-commerce. *Journal of Business Perspectives*, 18(4), 245–260.
- Yuniarti, F., R. Arief, H., Meydia, H., & Yevis, M. O. (2022). Online retailers' ethics and its effect on repurchase intention: The mediating role of perceived risk. *Cogent Business and Management*, 9(1). <https://doi.org/10.1080/23311975.2022.2051691>