Vol 8, Issue 3, 2025 **Impact Factor: 8.535** DOI: https://doi.org/10.31426/ijamsr.2025.8.3.8139

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Role of Cybercrime in Shaping E-Commerce Acceptance and Usage Patterns Among Consumers

Amshala Shankar [1]

[1] Research Scholar, Department of Law, P. K. University, Shivpuri, M.P., India.

Dr. Pankaj Kumar Mishra [2]

[2] Assistant Professor, Department of Law, P. K. University, Shivpuri, M.P., India.

ABSTRACT

Online shopping, digital payments, and reaching a wider audience have all contributed to e-commerce's prominence in today's economy. But many cybersecurity issues have surfaced with the digital transition, and cybercrimes have been on the rise, endangering companies and individuals alike. With an emphasis on the effects of cybercrime, this study investigates how chosen consumers in Hyderabad are familiar with, and make use of, e-commerce business technology platforms. We used a survey research methodology to collect data from 225 participants via a probability sampling technique. Of those, 180 responses were deemed legitimate and evaluated using descriptive statistics. According to the results, people still use e-commerce platforms, but they're wary of them because of the dangers they think cybercriminals pose. This makes them less likely to use them and has an effect on their adoption rate.

Keywords: *Business, Cybercrimes, Awareness, E-commerce, Technology.*

I. INTRODUCTION

When people purchase and sell products and services using online networks, this practice is known as electronic commerce (or "e-commerce"). Thanks to developments in internet access, the explosion of cellphones, and the growing dependence on digital payment methods, its expansion over the past 20 years has been unparalleled. The COVID-19 pandemic hastened this trend even more, as people resorted to buying online rather than in real stores due to social distancing measures and lockdowns. Consequently, online shopping soared to new heights, boosting economies around the world and providing companies with a means to tap into worldwide marketplaces regardless of their physical location.

Many positive outcomes have resulted from this shift to digital, including lower operational expenses, a wider audience reach, and an enhanced user experience as a result of more targeted advertising and better support. Consumers now find and buy things mostly through online marketplaces, mobile apps, and social media channels. On the other hand, companies are now more vulnerable to cyber threats that could compromise the security of their data, financial transactions, and availability.

When criminals use digital methods to commit their crimes, they are committing cybercrimes. Cybercrimes can affect any type of computer system, network, or data. Some examples of these crimes are virus attacks, ransomware, phishing, identity theft, and hacking. Cybercriminals see the proliferation of online shopping as an opportunity to steal personal information, financial data, and even intellectual property due to the easy access to large volumes of sensitive data stored in the digital realm.

When it comes to online shopping, identity theft is a major problem. In order to commit fraud or sell the information on the dark web, cybercriminals frequently take advantage of security holes in online platforms to get sensitive consumer data. Another prevalent approach is phishing, which involves creating fake emails or webpages in order to fool victims into giving their credentials. In addition to causing monetary losses, these actions undermine customer confidence in online marketplaces.

Malware is another major risk to online shopping since it can harm or steal data from computers. Businesses have been hit hard by ransomware attacks, a kind of software that encrypts important data and demands payment to decrypt it. Such attacks can cause major problems for online businesses, including interruptions in operations, harm to their reputation, and a decrease in client trust.

The strategies used by cybercriminals also change as technology does. Advanced cyber risks have emerged in recent years, including examples like supply chain attacks. In these attacks, hackers get indirect access to critical data by infiltrating the software or service providers of e-commerce enterprises. Since more and more companies are using cloud storage, payment processing, and customer relationship management systems provided by third parties, this has grown into a major worry. When one of these service providers has a security breach, it can expose all the organizations who rely on them, which can result in extensive data breaches.

II. REVIEW OF LITERATURE

Apau, Richard & Koranteng, Felix. (2020) The rate of cybercrime is rising rapidly in many economies. The main drivers have been the digitization of commercial activity and the fast expansion and adoption of the internet. Cybercrime is a persistent problem that affects people's willingness to shop online and the security of e-commerce platforms. This study explores the relationship between cyber-crime, trust, and users' intention to conduct business using e-commerce technologies. It does so in light of the increasing number of cyber-crime activities and the lack of research in this area, especially in developing nations. An online questionnaire was sent out to 476 individuals as part of the survey approach. The data was thoroughly examined using Partial Least Square Structural Equation Modelling. We find that the following factors significantly predict the desire to purchase using e-commerce technologies: trust in internet media, attitude towards behavior, subjective norm, perceived behavioral control, and cyber-crime beliefs. Results shed light on how consumers' views of trust and cybercrime affect their propensity to make a purchase, which is useful information for stakeholders and companies. The necessity to strengthen e-commerce platform security measures is further highlighted by this.

Apau, Richard et al., (2019) Access to worldwide markets, a competitive edge, and increased company effectiveness are the three main reasons why e-commerce technologies are seeing continued adoption and usage. Concerns about security and reliability have a significant impact on people's decisions to utilize and make use of e-commerce platforms. In light of the recent spike in cybercrime and the dearth of studies focusing on this topic, especially in developing nations, this paper sought to fill that knowledge gap by exploring the relationship between consumers' views of cybercrime and their propensity to engage in online commerce. The data from 476 participants was thoroughly examined using Partial Least Square Structural Equation Modelling. The data was collected using an online questionnaire that was distributed using a survey approach. Using trust and perceptions of cybercrime, the article expands the premise of reasoned action. Previous research served as the basis for the deductive reasoning that established the connections between the various constructions. A third of the variation in consumers' attitudes toward behavior and nearly half of the variation in their intentions to buy were accounted for by the proposed model. The results show that e-commerce intention is significantly predicted by cyber-crime beliefs, attitude towards behavior, subjective norm, and trust in online medium. Neither the Trust of Ecommerce Sellers nor the Cyber Crime Perceptions nor the Purchase Intention of Consumers were significantly related. The results shed light on the effects of trust and perceptions of cybercrime on consumers' intents to buy for businesses and other interested parties. Additionally, it motivates developers of e-commerce technologies to include security measures that make these systems less susceptible to attacks. Lastly, this study only included respondents from Ghana, so future research could expand to include samples from other nations.

Faisal, Abdullah & Ghouri, Arsalan. (2023) The goal of this research is to find out how important cybersecurity measures are for preventing cyberattacks on e-commerce platforms, particularly how strong the encryption is, the firewall settings, and the authentication methods. Information technology (IT) managers in Saudi Arabia who are in charge of e-commerce operations were surveyed as part of the data collection procedure. Out of 300 questionnaires that were distributed, 190 were chosen for analysis using a convenience sampling procedure. The model for measurement was calculated using Amos's structural equation model. It included variables including ES, FC, AP, security training, cyber-attack incidences, customer trust, and incident reaction time. This study's findings have important implications for understanding the nature and impact of cybersecurity measures on cyberattack frequency. The study emphasizes the importance of authentication mechanisms, firewall settings, and encryption in enhancing e-commerce platforms. The report also looks at how security training affects the overall cybersecurity posture, which in turn affects customer trust. The investigation also considers the amount of time it takes to respond to an incident, which is an important factor in reducing the impact of cyber disasters. A better understanding of the cybersecurity landscape in the e-commerce domain is enhanced by the results of this study. Organizations can enhance their cybersecurity strategies and protect themselves from new cyber threats by using the practical consequences of this research.

Setiawan, Nashrudin et al., (2018) There have been both beneficial and bad outcomes from the evolution of internet technology. The rise of cybercrime, particularly in the context of commercial business transactions, is one detrimental consequence. Customers' perceptions of online buying will be influenced by the impact. As a result, the company's online operations need to be vigilant against the potential risks associated with online transactions. In addition, in order to keep customers' trust in online buying and to reduce or eliminate risks, online businesses need to have the right plans and procedures in place. To ensure the security of customers' personal information and financial data when they shop online, measures were put in place to safeguard virtual transactions. Making sure customers are constantly satisfied and comfortable when purchasing online is another important purpose of the organization.

III. RESEARCH METHODOLOGY

Users of e-commerce platforms used by Hyderabadi businesses were the subjects of this research. The research strategy used in the study was a survey. Using a probability sampling technique, 225 participants were chosen at random. Respondents were asked to fill out and submit a closed-ended questionnaire; however, 20 of the 200 copies were filled out incorrectly, leaving a total of 180 replies that could be analyzed. Using face validity, the survey was shown to be valid. Using descriptive analysis, the collected data were examined.

IV. DATA ANALYSIS AND INTERPRETATION

Table 1: Gender of The Respondents

Particulars	Frequency	Percentage (%)
Male	75	41.67
Female	105	58.33
Total	180	100

There are 105 female respondents (58.33%) and 75 male respondents (41.67%), according to the data. It appears that a larger percentage of the participants are female, constituting over 50% of the whole sample.

Table 2: Awareness Level of E-Commerce Business Platform

Particulars	Agree %	Neutral %	Disagree %
Awareness of e-commerce business platform	91.0	7.0	2.0
An active user of e-commerce business platforms	82.0	10.0	8.0
At least a purchase through e- commerce business platforms	96.0	1.0	3.0
Usage of e-commerce business platforms require knowledge of IT	63.0	16.0	21.0
Usage of e-commerce business platforms is prevalent among young adults	75.0	16.0	9.0
Usage of e-commerce platforms for my purchases because it is more convenient	72.0	17.0	11.0
Receiving goods purchased through the online platform without delay	58.0	17.0	25.0

Table 2 reveals that although only 82% of people actually use these platforms, 96% have made a purchase through them, and 91% are aware of them. Nevertheless, when it comes to the requisite IT knowledge, attitudes are divided: 63% think it's vital, while 21% disagree. The majority of young individuals (75%) prefer to shop online, and even more (72%) say it's more convenient. Yet, just 58% are in agreement that things are delivered promptly, suggesting that there are some reservations regarding the dependability of delivery.

Table 3: Cybercrimes Perception and Usage of E-Commerce Business Technology Platforms

Particulars	Agree %	Neutral %	Disagree %	Mean	Std. Dev.
There is prevalence of cybercrimes	95.0	4.0	1.0	1.46	0.561
Acceptance of e-commerce business technology platforms is slow due to prevalence of cybercrimes	71.0	18.0	11.0	2.05	0.997
There is low usage of e-commerce business technology platforms due to the menace of cybercrimes	74.0	20.0	6.0	1.99	0.867
The usage of e-commerce business technology platforms has been greatly hampered due to cybercrimes	69.0	22.0	9.0	2.21	0.878
Users take precautions when buying on e-commerce business technology platforms	93.0	5.0	2.0	1.59	0.615
Users always verifies the genuineness of e-commerce business technology platforms before making payments due to prevalence of cybercrimes	91.0	7.0	2.0	1.51	0.646
Cybercrimes have negative effect on users of e-commerce business technology platforms	87.0	11.0	2.0	1.68	0.781
E-commerce business technology platforms is risky	82.0	14.0	4.0	1.91	0.920
Cybercrime activities poses threat to usage of e-commerce business technology platforms	90.0	7.0	3.0	1.78	0.808

Users have a high opinion of the cybercrime threats posed by e-commerce business technology platforms, according to Table 3. The overwhelming majority of people (95%) think that cybercrimes are common, and 90% think that these activities make these platforms less safe to use. Concerns about cybercrime have slowed the adoption of e-commerce platforms (71% reduction) and decreased their usage (74% decrease). Cybercrime concerns have also had a major impact on platform usage, according to 69% of respondents. Many users still take care, though; for example, 93% make sure to check the platform's legitimacy before making a payment, and 91% employ some sort of security protection when completing a purchase. Users attempt to control these risks through prudent procedures, according to the research, even if they are aware of them (82% see e-commerce as risky and 87% understand the negative effects of cybercrimes). In addition, the descriptive statistics revealed that the mean and standard deviation of the sampled users of e-commerce business technology platforms range from 1.46 to 2.18 and 0.561 to 0.997, respectively. This indicates that the responses vary moderately from one another, with values that are not too far from the mean.

V. CONCLUSION

Users of e-commerce platforms should always check the legitimacy of e-commerce platforms before proceeding with transactions, the government should enforce comprehensive cyber laws, anti-cybercrime agencies should be set up to make sure these laws are effectively put into place, and e-commerce platforms should have sufficient security measures to protect users from cybercriminals.

REFERENCES

1. Abdullah Faisal and Arsalan Ghouri, "Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-Commerce Platforms," Vol. 15, No. 2, *International Journal of eBusiness and eGovernment Studies*, 2023, pp. 444-469. DOI: 10.34109/ijebeg.2023150120.
2. Dr. Bhatt, "Impact of AI in E-Commerce: A Perception of Consumers of Ahmedabad," Vol. 10, No. 2, *International Education and Research Journal*, 2024, pp. 33-41. DOI: 10.21276/IERJ24846377766556.
3. Elizabeth Goldsmith and Sue Mcgregor, "E-Commerce: Consumer Protection Issues and Implications for Research and Education," Vol. 24, No. 2, *Journal of Consumer Studies & Home Economics*, 2008, pp. 124-127. DOI: 10.1046/j.1365-2737.2000.00150.x.
4. Juan Wijaya et al., "Shaping Trust and Loyalty in Online Commerce: An Empirical Study of Influential Factors," Vol. 101, No. 21, *Journal of Theoretical and Applied Information Technology*, 2023, 6871-6886.
5. Khaled Alshare, Murad Moqbel, and Mohammad Garni, "The Impact of Trust, Security, and Privacy on Individual's Use of the Internet for Online Shopping and Social Media: A Multi-Cultural Study," Vol. 17, No. 5, *International Journal of Mobile Communications*, 2019, p. 513. DOI: 10.1504/IJMC.2019.102082.
6. Latifa Albshaier, Seetah Almarri, and M. M. Rahman, "A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions," Vol. 13, No. 2, *Computers*, 2024, p. 27. DOI: 10.3390/computers13010027.
7. Latifa Albshaier, Seetah Almarri, and M. M. Rahman, "A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions," Vol. 13, No. 8, *Computers*, 2024, p. 27. DOI: 10.3390/computers13010027.
8. Mohammed Alhashem et al., "Exploring the Factors Affecting Online Trust in B2C E-Commerce Transactions in India: an Empirical Study," Vol. 08, No. 12, *International Journal of Professional Business Review*, 2023, pp. 1-29. DOI: 10.26668/businessreview/2023.v8i12.3945.
9. Moudi Almousa, "Barriers to E-Commerce Adoption: Consumers' Perspectives from a Developing Country," Vol. 05, No. 3, *iBusiness*, 2013, pp. 65-71. DOI: 10.4236/ib.2013.52008.
10. Nashrudin Setiawan et al., "Impact of Cybercrime in E-Business and Trust," *International* Vol. 9, No. 7, *Journal of Civil Engineering and Technology*, 2018, 652-656.

11. Richard Apau and Felix Koranteng, "Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behavior," Vol. 13, No. 2, *International Journal of Cyber Criminology*,2020, pp. 228-254. DOI: 10.5281/zenodo.3697886.
12. Richard Apau, Felix Koranteng, and Samuel Gyamfi, "Cyber-Crime and its Effects on E-Commerce Technologies,", Vol. 5, No. 1, *Journal of Information* , 2019, pp. 39-59. DOI: 10.18488/journal.104.2019.51.39.59.
13. Saqib Saeed, "A Customer-Centric View of E-Commerce Security and Privacy," Vol. 13, No. 10, *Applied Sciences*,2023, 1020. DOI: 10.3390/app13021020.
14. Sofik Handoyo, "Purchasing in the Digital Age: A Meta-Analytical Perspective on Trust, Risk, Security, and E-WOM in E-Commerce," Vol. 10, No. 3, *Heliyon*, 2024, e29714. DOI: 10.1016/j.heliyon.2024.e29714.
15. Zlatan Morić et al., "Protection of Personal Data in the Context of E-Commerce," Vol. 4, No. 3, *Journal of Cybersecurity and Privacy*,2024, pp. 731-761. DOI: 10.3390/jcp4030034.