

Letter to Editor

Online Purchase Intention and Cyber Frauds during COVID-19

Sayed Saiful Amin ^{1,*}¹ Faculty of Business, Accounting & Management, SEGi University, Malaysia.

*Correspondence: sydamin27@gmail.com

Abstract: The closure of physical stores due to lockdown and social distancing measures led consumers to ramp up online purchasing intention, which in turn accelerated global e-commerce market growth, but caution must be ensured to prevent cyber frauds.

Keywords: Online purchase intention; Cyber fraud; COVID-19

Corona pandemic is a worldwide disaster. To prevent the transmission of the virus, social distance is mandatory and mass gathering is a risky behavior. Moreover, maintenance of social distance is crucial as the number of new Covid-19 cases has been increasing at an exponential rate. Hence, implementation of stay home approaches is applicable at all levels which leads to the growth of e-commerce platforms including the consumer's online purchase intention globally. It is the best time to think for consumer's cyber security to mitigate the present calamity of their online purchase intention.

The severe repercussions of the COVID-19 pandemic have resulted in a painful economic recession across the globe [1]. Although it was projected that e-commerce trends will be escalating by 2023 [2] but restrictions and lockdowns have affected global supply chains, and hence seriously damaging the global economy [1]. Therefore, to boost the economic process, e-commerce is the best possible solution, where we might augment the consumer's online purchase intention by ensuring preventive measures on cyber frauds.

According to the Forbes report, retailers started to shrink their physical presence due to the shift toward online shopping [3]. The diffusion of the COVID-19 epidemic has influenced customer's online purchase intention and led to increased online shopping [4]. It might imply that consumers might not have any choice other than online shopping to stay away from physical stores and places to avoid crowds so to decrease the possibility of virus infection. Thus, it has become essential to understand the dynamics in customers' online shopping behaviors during the COVID-19 pandemic.

As the business environment has been moving towards a more digitally centered operation, organizations must consider the challenges and concerns in maintaining their security and business continuity. This digital world has become more at risk. Recent evidence suggests that cyber fraud is an emerging threat during this current pandemic crisis [5]. Organizations need to consider how to keep the business protected from attackers exploiting the uncertainty of the situation.

It is unclear how long this crisis will last and whether further shutdowns will be required in the future. Consumer behavior might change over the long term in response to the COVID-19 pandemic, and cyber security is crucial to ensure online purchase intention. To ensure that e-commerce can maintain the popularity it gained during the shutdown even after the reopening of stores, both political and corporate decision-makers

How to cite this paper: Amin, S. S. (2021). Online Purchase Intention and Cyber Frauds during COVID-19. *Universal Journal of Finance and Economics*, 1(1), 1-2. Retrieved from <https://www.scipublications.com/journal/index.php/ujfe/article/view/113>

Received: August 21, 2021

Accepted: August 25, 2021

Published: August 26, 2021



Copyright: © 2021 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

must be aware of the opportunities available to them in terms of shaping consumer behavior through communication strategies.

COVID-19 has made many sectors switch rapidly from traditional 'face-to-face' to virtual platforms. E-commerce service is not an exception, online purchasing has moved to a brighter spot than ever due to COVID-19 pandemic. However, cyber security threats including hacking, misuse of personal data, monetary theft, phishing attacks, unprotected provision of services, credit card frauds should be under strict monitoring to boost the consumer's online purchase intention during this global crisis of covid pandemic.

Funding: This research received no funding.

Conflicts of Interest: The author declares no conflict of interest.

References

- [1] Ebrahim, S.H.; Ahmed, Q.A.; Gozzer, E.; Schlagenhaut, P.; Memish, Z.A. 2020. Covid-19 and community mitigation strategies in a pandemic. *BMJ*, 368, m1066. <https://doi.org/10.1136/bmj.m1066>
- [2] Lipsman, A. 2019. Global ecommerce 2019. <https://www.emarketer.com/content/globalecommerce-2019> (Accessed July 2021).
- [3] Loeb, W. 2020. More than 15,500 stores are closing in 2020 so far—a number that will surely rise. <https://www.forbes.com/sites/walterloeb/2020/07/06/9274-stores-are-closing-in-2020-its-the-pandemic-and-high-debt-more-will-close/?sh=50742956729f> (Accessed July 2021).
- [4] Addo, P. C., F. Jiaming, N. B. Kulbo, and L. Liangqiang. 2020. COVID-19: Fear appeal favoring purchase behavior towards personal protective equipment. *The Service Industries Journal*, 40 (7–8):471–490. <https://doi.org/10.1080/02642069.2020.1751823>.
- [5] Ma, K.W.F. and McKinnon, T. 2021. COVID-19 and cyber fraud: emerging threats during the pandemic, *Journal of Financial Crime*, <https://doi.org/10.1108/JFC-01-2021-0016>