User's awareness of personal data leakage in E-commerce application

Raditya Andhikaputra [1], *Samuel Marc Anthony* Tumbel [1], *Jason* Vida[1], *Anderes* Gui[1*], *I Gusti Made* Karmawan[1], *and Yuvaraj* Ganesan[2]

[1] School of Information Systems, Bina Nusantara University, Jakarta 11480, Indonesia
[2] Graduate School of Business Universiti Sains Malaysia Penang, Malaysia

Abstract. Our daily lives now involve e-commerce, and because of how convenient it is to use them, e-commerce apps are becoming more and more common. Accessibility and convenience do, however, come with concerns about personal data leakage. The term "personal data leakage" refers to the unlawful sharing of personal information that can be utilized for negative purposes like fraud or identity theft. This paper is aimed at investigating the awareness of personal data leakage among users of e-commerce apps. Using convenience sampling methods to collect data. A survey was conducted with 566 respondents who used e-commerce apps at least once. The aim of the study was to determine how well respondents understood the elements that influence the security of online transactions in e-commerce. The study's findings indicated that most participants are aware of the dangers of disclosing personal information online. Moreover, users of e-commerce applications should pay more attention to privacy concerns and safe online transactions in order to increase user privacy concerns and the application's ability to conduct secure transactions. The results of this study point to the necessity for e-commerce app developers to play a more active role in informing their users of the value of data privacy and the precautions they may take to safeguard their personal data.

1 Introduction

Global e-commerce is encouraged and given opportunity by the rising number of Internet users around the world. The digital age shows rapid movement, providing business opportunities for individuals to be able to reach a larger market from anywhere around the world. E-commerce, which is considered the most important platform that should be maximized, offers special characteristics that help people in the promotion and sale of products online [1]. In Indonesia, the e-commerce industry has experienced significant progress in recent years. The rapid growth of the middle class, the level of internet penetration has increased, the explosive growth of information technology and the capacity to store and process large amounts of personal information have gone hand in hand with the increase in internet usage and the popularity of mobile devices have created a favorable environment for e-commerce businesses. According to a research from Google, Temasek, and Bain & Company, Indonesia's e-commerce market would reach $124 billion by 2025, with a 25% annual growth rate [2]. Several causes, such as the introduction of online marketplaces, the rise of logistical networks, and the acceptance of digital payments, are responsible for this growth. However, the industry still faces various challenges, including logistics issues, payment infrastructure, and regulatory frameworks.

Despite the progress of e-commerce as an online platform for electronic services, with its development comes security risks that can interfere with the comfort of a person in making transactions. One of the security risks that arise is privacy concerns. Due to technology advancements that make it simple for unauthorized parties to gather, store, and distribute a person's personal information, this subject has recently gained more and more public attention in the contemporary digital era. However, the development of the internet and social media has raised public concerns about privacy because it is so simple to upload and distribute personal information publicly without the owner of the information being aware of it. According to Baek and Morito, when a person reaches a certain level of privacy concern, they begin to worry that their right to protect their personal information may be violated [3]. Several factors, including but not limited to unauthorized access, secondary use, interception of personal information, and inappropriate handling of such information, might lead to user privacy issues [4]. Privacy issues therefore become crucial when customers perform online transactions that call for financial and personal

* Corresponding author: anderesgui@binus.edu

information. Customers view providing such information as dangerous since it may be risky and vulnerable to future and opportunistic acts of businesses.

There are several things that affect the impact on Privacy Concern in E-Commerce, specifically the Internet in relation to these two characteristics since it was mentioned in a prior study that people with higher self-efficacy may find it more difficult to conduct transactions online sometimes. Internet self-efficacy is the term for a person's appraisal of his own competence to engage with the internet, according to studies discussed by various experts. A person's perceived self-efficacy is their belief in their capacity to use technology or mobile devices to carry out specific activities [5]. And also the relationship might try more things and gain more knowledge. A person's belief in their "abilities to plan and carry out the steps necessary to reach a particular degree of performance [6]. Higher self-efficacy levels are associated with greater self-assurance in one's capacity to accomplish a variety of online tasks, including privacy management.[6].

Privacy awareness and privacy concern are closely related concepts in the digital age. Privacy awareness is the knowledge and understanding of one's privacy rights and the risks of disclosing personal information online, while privacy concern is the level of fear or anxiety one has about their personal information being accessed, used or shared without their consent. When people are more aware of their privacy rights, they are more inclined to voice their privacy concerns, whereas those who are less aware of these hazards may be less likely to do so. The level of privacy awareness is the degree to which people are aware of their rights to privacy and the potential repercussions of releasing personal information online. According to Acquisti, Because it affects how much personal information people are willing to share, how much they are willing to pay for privacy-enhancing tools, and how likely they are to engage in privacy-enhancing behaviors, privacy awareness is a crucial factor in how people behave and make decisions regarding their privacy [7]. The relationship between the two is not always direct, Acquisti also point out that there are other factors, such as personal beliefs, cultural norms, and situational considerations, that can affect a person's level of privacy concerns, which complicates the relationship between privacy awareness and concerns [7]. However, the ongoing debate about data privacy and the ways in which individuals can protect their own information in an increasingly interconnected society should take privacy awareness and concern into account.

Technological changes affect the involvement or social participation of users today. Kim found that the sense of belonging of each customer there is a relationship of interaction with inter-net users especially brands belonging to e-commerce and seen from the negative side with customer engagement component of the possibility of mistaken purchases [8]. Can create engagement for consumers in online shopping groups for consumers and a strong intention to buy from online shopping group websites [8]. Zaichkowsky defines engagement as "the relevance a person feels toward an object based on his or her inherent needs, values, and interests" when discussing the definition of engagement in general [6]. So, with the internet leading to social relationships which can connect people or subjects to engage with products/objects, namely using the internet in order to join together in a community from the basis of common interests.

With its rapid evolution, large number of applications, as well as a wealth of information resources, and global reach to homes, the internet has given people to use the internet in a variety of ways and purposes. Namely entertainment, education, information seeking, and communication. According to Andrews, internet use will be motivated by engagement, and individuals will discover that they use it for a variety of reasons and at various frequency [6]. Interaction with products has been researched by Cass (2000) in the past because when we think of products or things, there is a special place occupied in their lives. It's something quiet learning functionalities and product requirements. People today use the internet in a variety of ways, some so that the internet can provide benefits, to improve technical skills, there are also social contacts through communication by interacting to provide information via email, distribution lists, chat, and similar applications. At this time, consumer interaction with one of the products that is widely done is e-commerce. In e-commerce, many users carry out commercial transactions, for example for household needs. Because many use e-commerce applications, this causes problems such as attacks or fraud and data theft to increase. Therefore, along with the increasing number of user involvement in using and knowing about the internet, It will instill confidence in each user, enabling them to better handle sharing sensitive information online. They'll be able to engage and transact safely since they'll be aware of which applications and people they may give their information to.

This paper aims to examine what factors influence e-commerce app users' awareness of personal data leakage, include users' responses to online privacy/personal data leakage issues among Indonesian e-commerce users.

2 Hypotheses development

2.1 Internet self efficacy

Internet Self-Efficacy (ISE) is the self-evaluation of a person's ability to interact with the Internet. [9]. Bandura brings up self-efficacy, or confidence in one's capacity to carry out specific behaviour. Self-efficacy affects decisions on the behaviours to engage in, the effort and tenacity expended to engage in those behaviours in the face of difficulties, and ultimately, the degree to which such behaviours are mastered. [10]. (Mohamed and Ahmad) demonstrated a positive association between self-efficacy and motivation to protect information online. Self-efficacy had an impact on the intention to follow advised preventive health behaviour recommendations, the level of privacy concerns for personal information, the usage of decision-support tools, and the desire to implement anti-virus behaviours. Users take part in securing their environment on the internet when they perceive danger and feel confident

that they have the knowledge and skills to avoid or deal with it. As a result, they may enable privacy controls on social networking sites. Therefore, users with high levels of self-efficacy When utilizing privacy settings on e-commerce applications, users frequently have their own personal data security as their first priority. [11].

Internet self-efficacy (ISE) is the ability to plan and carry out Internet-related activities in a way that yields the desired results. As online transactions increase, it is crucial to take Internet self-efficacy into account as a predictor of success in those transactions, As online learning expands, it is crucial to take Internet self-efficacy into account as an indicator of academic achievement. [9]. Additionally, numerous prior research in a variety of technological contexts have confirmed the impact of Internet Self-Efficacy on Safe Online Transactions [6].

H1: Internet self-efficacy has a positive impact on privacy concern.

H2: Internet self-efficacy has a positive impact on Safety Online Transaction E-Commerce.

2.2 Privacy awareness

To mitigate information security issues, it is imperative to understand PA and its causes. Employees' level of understanding of the significance of the information security policies, rules, and guidelines implemented by their business, as well as their level of adherence to those policies, rules, and guidelines, is referred to as their level of privacy awareness (PA), In the context of Privacy Awareness (PA), It has been employed the Knowledge, Attitude, and Behavior (KAB) model. This strategy contends that employees' attitudes improve as their understanding of security behaviors grows, and that this results in enhanced information security behaviors [12]. Given the public character of cyberspace, research on privacy issues in the context of social media has revealed a negative correlation between profile visibility, personal information exposure, self-disclosure, and self-expression. [13]. Moreover, the influence of Privacy Awareness on Privacy Concern Practices has been validated in many previous studies in various technology contexts [14].

H3: Privacy awareness has a positive impact on privacy concern practices.

2.3 Internet social involvement

Internet Social Involvement (ISI) is level of involvement in a group or society is referred to as social engagement (sometimes spelled social involvement or social participation) [15]. Yang (2012) defines engagement as "an opinion about an engagement association. According to requirements, principles, and personal interests" [15]. Because of their engagement, more people will use the internet, and they will do so more frequently and for different reasons [6]. According to Zaickowsky, individual-related characteristics, environment-related factors such as brand familiarity, and circumstance-related factors are all key indicators of engagement [15]. Social media usage and online networking are just two examples of activities that fall under the category of social engagement on the internet. Privacy concerns have also become more prevalent with the increased use of internet platforms. So, the possible hypothesis is that as internet social interaction increases, privacy concerns among internet users will increase. This theory is predicated on the notion that individuals who participate in more social interactions online will be more cognizant of potential privacy dangers and, hence, more thermo-activated to safeguard their personal information online. Such people may be more cautious about the data they disclose online and may be more likely to take precautions to protect their privacy [16]. The kind of social networking activities that people engage in could also operate as a mediator between online social interaction and privacy worries. Specifically, participating in more privacy-sensitive activities may be associated with higher concerns, whereas participating in less sensitive activities may be associated with lower privacy concerns [17]. Overall, understanding how people perceive and manage their online privacy depends on looking at the relationship between social engagement on the internet and privacy concerns. Such studies can provide perspectives on how online platforms can be made to protect users' privacy more effectively and reduce privacy risks. Therefore, we propose the following:

H4: Internet social involvement has a positive impact on privacy concern.

2.3 Privacy concern practices

Privacy Concern Practices (PCP) is concern over how others might use personal information about people is what it's talking about [16]. Consumer shopping has been revolutionized by e-commerce, and privacy concerns are now a key determinant of online transaction behavior. Data breaches, data misuse, and online fraud are just a few examples of the many situations that privacy concerns can arise. These concerns can negatively impact consumer trust in e-commerce websites and result in a decrease in online transaction activity. Youn (2009) states that the lack of clarity regarding customer information and who has access to it impacts information security and privacy [18]. In shopping on e-commerce because using the internet to make transactions does require sharing personal information. So, it is all an important concern among consumers, the protection and legitimate use of such information. But often users do not really know whether their personal information will be used as Rapp [18]. Online transaction security and privacy concerns are positively related, as consumers who perceive higher levels of online security also tend to have lower levels of privacy concerns in e-commerce transactions. Consumers who have higher levels of privacy concerns are less likely to engage in online transactions in e-commerce. This is supported by research that indicates that social media is often considered a less secure environment for online transactions due to the potential for data breaches and identity theft.

H5: privacy concern has a positive impact on safety online transaction e-commerce.

The research framework is described in Figure 1.

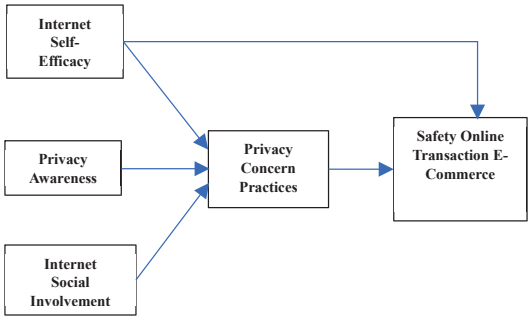

Fig. 1. Research Framework.

3 Research methodology

3.1 Data collection

The users of the E-commerce applications in Indonesia as unknown population. Minimum sample for unknown population is 385. A questionnaire with 6-point Likert scales (6- very strongly agree, 1- very strongly disagree) is used to collect data. The survey was broken up into various sections. The first section of the questionnaire asks for demographic information such name, age, gender, education level, and place of residence. Part 2: Frequency of E-Commerce Use (Have You Ever Used an E-Commerce, How Often Have You Used an E-Commerce, How Often Have You Used an E-Commerce Platform). The target respondents are Indonesians who use e-commerce applications and are primarily from Greater Jakarta. Data were gathered through purposive sampling between April and May 2023.

3.2 Data analysis method

Using path coefficients, the analytical approach uses SmartPLS 4.0 to examine the convergence validity, discriminant validity, and hypothesis testing.

4 Result and discussion

Demographic data from survey respondents is shown in Table 1. Majority of respondents from Z and Y generation, majority with education Bachelor degree, majority of respondent live in Greater Jakarta. Majority of respondent using e-commerce less than 4 times per week.

Table 1. Demographics respondents.

Category	Description	Freq.	Percentage
Gender	Male	284	50.18%
	Female	282	49.82%
Age	17-25 Years	255	45.05%
	26-41 Years	178	31.45%
	42-57 Years	81	14,.1%
	58-63 Years	20	3.53%
	>63 Years	25	4.42%
Level of Education	Up to High School	57	10.07%
	Diploma	103	18.20%
	Bachelor	332	58.66%
	Master	64	11.31%
	Doctoral	3	0.53%
Domicile	Jakarta	161	28.45%
	Bogor	96	16.96%
	Depok	81	14.31%
	Tangerang	88	15.55%
	Bekasi	69	12.19%
	Others	71	12.54%
E-commerce Usage	1-3 times per week	325	57.42%
	4-6 times per week	178	31.45%
	> 6 times per week	63	11.13%

Table 2. Convergent validity.

Variables	Item	Outer Loading	CR	AVE
ISE	ISE1	0.669	0.785	0.550
	ISE2	0.691		
	ISE3	0.711		
	ISE4	0.722		
ISI	ISI1	0.829	0.840	0.724
	ISI3	0.872		
PA	PA1	0.702	0.829	0.548
	PA2	0.772		
	PA3	0.724		
	PA5	0.619		
	PA6	0.690		
PCP	PCP1	0.687	0.875	0.539
	PCP2	0.735		
	PCP3	0.776		
	PCP4	0.765		
	PCP5	0.734		
	PCP6	0.703		
SOTE	SOTE1	0.655	0.817	0.527
	SOTE2	0.631		
	SOTE3	0.702		
	SOTE4	0.714		
	SOTE5	0.697		
	SOTE6	0.603		

Table 2 measures several measurement-related constructs and consider the variance of the elements of the construct. It shows outer loading to check the convergent validity of each concept measure, outer loading is the correlation between indicators and their constructs. Indicators that have insignificant weights should be removed if the loading is also insignificant according to Hair (2017). if the indicator has a low but meaningful weight of 0.50 or below, the indicator should be removed unless the measurement theory strongly supports its inclusion. Metrics used to evaluate the construct's convergent validity, such as AVE/ average

variance extracted, with an acceptable AVE value of at least 0.50 [19].

Table 3 evaluates discriminant validity, or how much a construct differs experimentally from other constructs in terms of how well respondents can identify variations in other items and structural model meaning, according to Henseler (2015) for the assessment of discriminant validity performs well, proposing the HTMT of correlations; see also Voorhees (2016) for more information. The geometric mean of the average item correlations across constructs (i.e., heterotrait-heterometric correlations) divided by the average value of the item correlations for items measuring the same construct (i.e., monotrait-heterometric correlations) is known as HTMT. To determine a lower threshold value such as 0.85 or 0.90. And it needs to be checked if the value above 0.90 will indicate that the discriminant validity does not exist [19].

Table 3. Discriminant validity**.**

Variables	ISE	ISI	PA	PCP	SOTE
ISE					
ISI	0,367				
PA	0,648	0,085			
PCP	0,516	0,078	0,862		
SOTE	0,604	0,477	0,321	0,248	

Table 4. Path coefficient

Item	StDev	t-value	p-value	Decision
ISE -> PCP	0.04	2.769	0.003	Accepted
ISE -> SOTE	0.06	6.744	0.000	Accepted
ISI -> PCP	0.04	0.277	0.391	Rejected
PA -> PCP	0.04	17.620	0.000	Accepted
PCP -> SOTE	0.05	1.115	0.132	Rejected

The iterative PLS-SEM algorithm is used in this model's coefficient path modeling process, as seen at Table 4. Because it calculates the coefficients for the measurement model's and the structural model's partial least squares regression models [20].

5 Conclusion

With the development of technology over time, most people right now use e-commerce as a shopping tool for daily activities or requirements, because the process of e-commerce is so digitalized and easy access to many e-commerce application users. The association between Internet Self-Efficacy, Privacy Awareness, Internet Social Involvement, Privacy Concern Practices, Safety Online Transaction, and E-Commerce is examined in this study, From Table IV, Each hypothesis' outcome is visible. Internet Social Participation and Privacy Concerning Behavior, and the Relationship Between Privacy Concerning Behavior and Safe Online Transactions The finding is disregarded because e-commerce is not robust enough; this is linear with the prior study. The rest of the hypotheses like Internet Self Efficacy to Privacy Concerns Practices, Internet Self Efficacy to Safe Online E-commerce, and Privacy Awareness to Privacy Concerns Practices is accepted, As a result, when using an e-commerce application, users should pay more attention to privacy concerns and safe online transactions in order to increase user privacy concerns and the program's ability to conduct secure transactions. This study can be used as a resource for the developers of programs for them to consider how they can raise user privacy concerns and improve the security of online transactions, This study can be used as a resource for the developers of programs for them to consider how they can raise user privacy concerns and improve the security of online transactions.

6 Limitation and further study

Due to the deadline that was set, this study could not have been completed in the allotted time. The simple framework model was used because it would produce more relevant results given that participants' perceptions of safe online transactions, privacy concerns, and Internet self-efficacy, privacy awareness, and social involvement varied. Future research should be conducted based on a more explanation to give better insight into the trend of the safe online transaction to e-commerce application users privacy concern. The research scope can be increased by including a theory relevant to the variables related to the framework model that was used in this research. For the recommendation to future researchers who are investigating this variables, for the data to be more conclusive they need more time more than 3 months because there is a lot more variable that relates to the E-commerce phenomenon in Indonesia and also more respondents so that the data will be more concluded and more valid to discuss the relationship between each variables because in our research result in Table 4. Path coefficient the relationship between internet social involvement to privacy concerns practices and privacy concern practices to safe online transaction ecommerce resulted in negative or rejected decision we hope for future researchers to find more result to prove the decision if can be resulted as accepted in the path coefficient if they have more time and more respondents to gain more validity from the data analysis result. So that from both sides the e-commerce application users and the e-commerce application developers can reach an agreement between the internet social involvement, privacy concern practices and safe online transaction in e-commerce will be resulted as an positive impact between both sides of an e-commerce application.

Acknowledgement

This work is supported by Research and Technology Transfer Office, Bina Nusantara University.

References

[1] W. Wresch and S. Fraser, “Persistent Barriers to E-commerce in Developing Countries,” *J.*

Glob. Inf. Manag., vol. 19, no. 3, pp. 30–44, 2011, doi: 10.4018/jgim.2011070102.

[2] Google, Temasek, and Brain&Company, "e-Conomy Sea 2020 At full Velocity: Resilient and Racing Ahead," *J. Phys. A Math. Theor.*, vol. 44, no. 8, pp. 1–8, 2020, [Online]. Available: https://economysea.withgoogle.com/%0Ahttp://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1016/j.matlet.2019.04.024%0Ahttps://doi.org/10.1016/j

[3] T. Baek and M. Morimoto, "Stay away from me," *J. Advert.*, vol. 41, no. 1, pp. 59–76, 2012, doi: 10.2753/JOA0091-3367410105.

[4] C. Mutimukwe, E. Kolkowska, and Å. Grönlund, "Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior," *Gov. Inf. Q.*, vol. 37, no. 1, p. 101413, 2020, doi: 10.1016/j.giq.2019.101413.

[5] S. Singh, I. A. Zolkepli, and C. W. Kit, "New wave in mobile commerce adoption via mobile applications in Malaysian market: Investigating the relationship between consumer acceptance, trust, and self efficacy," *Int. J. Interact. Mob. Technol.*, vol. 12, no. 7, pp. 112–128, 2018, doi: 10.3991/ijim.v12i7.8964.

[6] S. H. Akhter, "Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement," *J. Consum. Mark.*, vol. 31, no. 2, pp. 118–125, 2014, doi: 10.1108/JCM-06-2013-0606.

[7] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age," *New Electron.*, vol. 40, no. 16, 2015.

[8] V. M. Sharma and A. Klein, "Consumer perceived value, involvement, trust, susceptibility to interpersonal influence, and intention to participate in online group buying," *J. Retail. Consum. Serv.*, vol. 52, no. September 2019, p. 101946, 2020, doi: 10.1016/j.jretconser.2019.101946.

[9] D. R. Compeau and C. A. Higgins, "Computer Self-Efficacy: Measure And Initial Development Of A Test," *MIS Q.*, vol. 19, no. 2, pp. 189–211, 2017, [Online]. Available: https://www.astm.org/Standards/E2368.htm

[10] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Comput. Human Behav.*, vol. 28, no. 6, pp. 2366–2375, 2012, doi: 10.1016/j.chb.2012.07.008.

[11] Y. C. Kuo, A. E. Walker, K. E. E. Schroder, and B. R. Belland, "Interaction, Internet self-efficacy, and self-regulated learning as predictors of student satisfaction in online education courses," *Internet High. Educ.*, vol. 20, pp. 35–50, 2014, doi: 10.1016/j.iheduc.2013.10.001.

[12] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput. Secur.*, vol. 88, p. 101640, 2020, doi: 10.1016/j.cose.2019.101640.

[13] T. R. Choi and Y. Sung, *Instagram versus Snapchat: Self-expression and privacy concern on social media*, vol. 35, no. 8. 2018. doi: 10.1016/j.tele.2018.09.009.

[14] L. N. Zlatolas, T. Welzer, M. Heričko, and M. Hölbl, "Privacy antecedents for SNS self-disclosure: The case of Facebook," *Comput. Human Behav.*, vol. 45, pp. 158–167, 2015, doi: 10.1016/j.chb.2014.12.012.

[15] C. McClure and Y. K. Seock, "The role of involvement: Investigating the effect of brand's social media pages on consumer purchase intention," *J. Retail. Consum. Serv.*, vol. 53, no. September 2018, p. 101975, 2020, doi: 10.1016/j.jretconser.2019.101975.

[16] T. Dinev and P. Hart, "PRIVACY CONCERNS AND INTERNET USE – A MODEL OF TRADE-OFF FACTORS," *Acad. Manag. Proc.*, no. 2000, pp. 1–7, 2006.

[17] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006, doi: 10.1287/isre.1060.0080.

[18] Y. C. Tsai and J. C. Yeh, "Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products," *African J. Bus. Manag.*, vol. 4, no. 18, pp. 4057–4066, 2010, [Online]. Available: http://www.academicjournals.org/AJBM

[19] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011, doi: 10.2753/MTP1069-6679190202.

[20] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "The Results of PLS-SEM Article information," *Eur. Bus. Rev.*, vol. 31, no. 1, pp. 2–24, 2018.