INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 10, (2024) E-ISSN: 2222-6990

Factors that Enhance Consumer Self-Protection Against Online Shopping Scams

Theppan Balakrishnan & Elistina Abu Bakar

Department of Resources Management and Consumer Studies, Faculty of Human Ecology

Corresponding Author Email: elistina@upm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i10/23323 DOI:10.6007/IJARBSS/v14-i10/23323

Published Date: 15 October 2024

Abstract

This study uncovers the factors that empower consumers to protect themselves against online shopping scams. The survey aimed to establish a significant relationship between self-efficacy, social influence, and awareness towards consumer self-protection. A quantitative method was adopted, and a self-administered questionnaire was used for data collection. The data was analysed using the Software Package for Social Science (SPSS). The analysis revealed that self-efficacy and awareness play significant roles in combating online shopping scams. At the same time, social influence was ineffective in enhancing consumer protection against online shopping scams. Both factors can explain 14.7% of the consumer's self-protection against online shopping scams, highlighting the empowering nature of awareness as the main predictor of self-protection. The results indicate that consumers can confidently shield themselves if they possess awareness and self-efficacy and are not controlled by social pressure like their peers. This study, therefore, serves as an empowering framework to boost consumer protection in Malaysia. The findings of this research provide consumers with a sense of control and confidence and can also help consumer associations and the government to increase consumer awareness programs in Malaysia.

Keywords: Consumer, Self-Protection, Self-Efficacy, Awareness, Online Shopping Scams

Introduction

Online scams and deceptive schemes orchestrated through the internet are a growing concern. These scams exploit the anonymity and reach of the digital world to manipulate victims into disclosing personal information, transferring money, or downloading malicious software (Nataraj-Hansen, 2024). The proliferation of internet use and digital transactions has led to various online scams, posing significant cybersecurity and personal privacy threats. In this paper, we narrow our focus to a specific type of online scam that is particularly prevalent: online shopping scams. These scams typically involve fraudulent online stores or fake listings that deceive consumers into purchasing non-existent or misrepresented products. Common cases include fake websites, counterfeit goods, and non-delivery of purchased items (Reurink, 2018).

Scams have existed since the inception of e-commerce, but the surge in online shopping during the COVID-19 pandemic created new opportunities for scammers. In 2020, online shopping scams made up 38 per cent of all reported scams globally, a significant increase from 24 per cent before the pandemic (Statista, 2022). Security breaches continue to heavily impact the industry, with losses from online payment fraud surpassing 40 billion U.S. dollars in 2022 (Statista, 2022). In Malaysia, 98,607 online fraud cases involving losses totalling RM3.3 billion were reported nationwide from 2017 until 2021 (Ministry of Communication, 2024). As of September 2023, there were more than 8,800 reports about online shopping scams in Malaysia (Statista, 2024). Internet scam misdeeds have a massive effect on victims, although the suspect and victim generally do not meet each other face-to-face (Alzghoul et al., 2024).

This study draws upon research on the factors that enhance consumer self-protection against online shopping scams. Identifying the factors that enhance consumer self-protection is essential to reduce the number of victims, particularly online shopping scams. The factors explored in this research were self-efficacy, social influence and awareness. Self-protection is essential as the Government agencies or the authorities involved will not always be available to protect consumers from scammers, and it is the responsibility of the consumers to protect themselves from scammers, mainly through online mediums.

Literature Review

Consumer protection has increasingly become critical with the rise of digital commerce, changing consumer behaviours, and global challenges like the COVID-19 pandemic. From 2020 to 2024, significant research focused on enhancing consumer rights, safeguarding data privacy, and adapting to new market conditions (Igbinenikaro & Adewusi, 2024). According to ASEAN (2018), consumer self-protection refers to the measures the consumers take to secure and advance their well-being and/or monetary interface. Consumer self-protection measures, such as consumer education, ensure that consumers can make well-informed choices and that suppliers fulfil their promises regarding the goods and services they offer, including those purchased online.

Due to the increasing number of online scams, consumer self-protection is important, especially when purchasing or doing any business online. Consumers in the present-day market economy regularly encounter data asymmetry and a critical awkwardness of bargaining control, particularly through the Internet (Brenncke, 2024). Therefore, online shoppers should be empowered by practising self-protection. For instance, those who are aware of their rights and responsibilities should always verify the details of the goods and services they intend to purchase, investigate the background of the online seller, and refrain from committing to any agreement before fully understanding the terms and conditions or providing personal information easily (Dol et al., 2015). These practices align with the National Consumer Policy (NCP), which emphasises that consumers who practise self-protection are smart, proactive, responsible, and capable of safeguarding themselves in the marketplace (Daud et al., 2020).

Self-Efficacy

Self-efficacy had a history that began with Bandura’s (1977) Social Learning Theory, which was relabelled as Social Cognitive Theory in 1986. One of Bandura’s vital ideas in his theory is self-efficacy. Bandura (1995) claimed that self-efficacy changes how people feel, think, act, and motivate themselves. Self-efficacy is not a perceived skill; it is what a person believes he or she can do with his/her skills under specific circumstances. It is not concerned with an individual's convictions around his/her capacity to perform particular and trifling acts but with convictions around his/her capacity to facilitate and organise aptitudes and capacities in changing and challenging circumstances (Bandura, 1994).

In the context of online shopping scams, self-efficacy plays a crucial role in determining a person's susceptibility to fraudulent schemes. This literature examines the link between self-efficacy and vulnerability to scams, focusing on how low self-efficacy can increase compliance with scam tactics and how scammers exploit this psychological trait (Nagin & Paternoster, 1993). Scammers are adept at identifying and exploiting low self-efficacy in their targets. They often use techniques that overwhelm and confuse, reducing the victim's self-efficacy. By creating a sense of urgency or fear, scammers can impair their target's ability to think critically and make informed decisions (Wikström & Kroneberg, 2022). Various methods can reduce self-efficacy, and scammers seem aware of this phenomenon.

Studies on self-efficacy have contributed enormously to our understanding of how consumers direct their own behaviour to prevent themselves from becoming victims of online fraud (Daud et al., 2020; Nawi et al., 2023). Based on these studies, self-efficacy is perceived as a factor that can enhance consumer self-protection against online scams, and it depends on individuals to protect themselves rather than on others to protect them.

Awareness

Ellis and Tucker (2009), defined awareness as the person's common hazard scale and information towards a condition or truth. These involve their awareness of purchasing online goods in business-to-consumer environments (Mariyappan & Sangeetha, 2024). In adapting to the cyber risk scene, cybersecurity awareness is fundamental for web users like youths as a counter-measure procedure to combat scammers' attacks (Rakin et al., 2024). The note of awareness must be compelling and ought to address all ages (Blackwood-Brown et al., 2021). It is additionally imperative to guarantee that the message of awareness is well-conveyed and that all significant groups get satisfactory consideration (Johri & Kumar, 2023), including youth and educated consumers such as university students (Dol et al., 2015).

Numerous analysts have claimed critical methods to present cybersecurity awareness since it is one of the best prerequisites of the internet community nowadays (Ridho, 2024; Burton et al.,2022). Due to its broad meaning, some researchers have operationalised awareness as threat awareness and coping awareness (Martens & De Marez, 2019). Threat awareness focuses on knowing what threats exist while coping awareness focuses on what security measures could be used to counter these threats (Hanus & Wu, 2016).

The definitions above show that awareness takes part in two significant ways, which are warning online clients of cyber security concerns and dangers and upgrading consumers' perception of online frauds so they can be completely motivated to grasp safety and enhance their self-protection (Zwilling et al., 2022). Online shopping scam awareness is not expecting panic or dread among consumers but getting ready for them to have a better plan against internet fraud. It is additionally a suitable stage to spread information concerning online scams. Sarno and Black (2024) found that digital literacy and cognitive reflectiveness can predict widespread vulnerability to online deception. Thus, awareness is an important determinant in predicting consumer self-protection.

Social influence

The culture, social class, reference group, family, and household of society all greatly affect how people behave (Wood, 2000). Wong (2019), referred to peer, parental, and media influences as social influences. Consumer behaviour is influenced by those around them (Andrei & Veltri, 2024). People frequently cling to social norms to understand and respond viably to social circumstances, particularly in times of helplessness (Ridho, 2024).

There are adequate studies that indicate that people are vulnerable to social influence (Yazdanmehr et al., 2020). People in various cultures establish their self-worth through differentiation from others in class (Markus & Kitayama, 1991). In criminology, crime rates can be clarified by the states of mind that society has towards wrongdoings (i.e. people are more likely to commit crimes if they accept that crime is common in their circle (Wang et al., 2021). If social influence tactics are employed in scams, individuals more susceptible to such influence may be more prone to complying with scammers' demands, ultimately to their detriment (Sharma et al., 2022). Based on this literature review, there is a need to understand whether social influence is considered a factor in enhancing consumer self-protection against online shopping scams.

Methodology

The researchers adopted an exploratory design to capture the paper’s objectives. This paper's choice of exploratory design enhances, supports, and provides an adequate understanding of the phenomenon. Quantitative techniques are applied to investigate the association between variables as this procedure can reflect the link in numbers and scientifically across the analysis. The respondents of this research were Universiti Putra Malaysia (UPM) students, meaning they were above 18 years old and perceived to have more knowledge and awareness regarding online shopping scams. UPM students were chosen because they represent university students from various backgrounds, genders, and age groups. UPM has 25,500 Malaysian and international students from more than 80 countries around the world. Roscoe (1975) recommended that the rule of thumb for choosing a suitable sample size is a minimum of 30 and below 500. Thus, 150 samples were chosen through a simple random sampling method, which fulfilled the minimum requirement.

The questionnaire has been divided into four sections: Section A deals with the participants' background information; Section B deals with self-efficacy; Section C deals with awareness; Section D deals with social influence; and Section E deals with the dependent variable of consumer self-protection practices. A five-point Likert scale, where (1) Strongly Disagree to (5) Strongly Agree, measures all the variables. Self-efficacy items were adopted from Chan and Lu (2004), and awareness items were derived partially from Luu, Land and Chin (2017), for the first three questions. The last two questions were derived from Dangi and Yacob (2013). The respondents answered questions on social influences adapted from Modic (2012) for all five questions. The questions for consumer self-protection practices were self-developed based on the information derived from the official website of the Royal Malaysian Police (2020), on tips to protect consumers against scams. The Cronbach Alpha value for self-efficacy was 0.893, social influence was 0.606, awareness (0.879) and consumer self-protection (0.726). Based on the value obtained, all the variables were proven reliable, with a value of 0.60 and above. The data was analysed using SPSS (Statistical Package for Social Science, 2022) utilising multiple regression analysis. From the above discussion, H_o1 was formulated.

H_o1: There is no significant relationship between self-efficacy, awareness, social influence and consumer self-protection practices.

Finding and Discussion

Four demographic characteristics were collected from the respondents: gender, age, ethnicity, and education level. Based on the data presented in Table 1, the percentage of male respondents was (51.3%), which was slightly higher compared to female respondents (48.7%). The dominant age in this study was 22-25 years old (72.7%), followed by 18-21 years old (17.3%) and 26-29 years old (10%). Many respondents were Indian (46%), followed by Malay (41.3%), Chinese (6%) and others (6.7%). Lastly, the data showed more undergraduate students (71.3%) than post-graduate students (28.3%).

Table 1
Demographic background of respondents

Variable	**Respondent Information**	**Frequency n=150**	**Percentage (%)**
Gender	Male	77	51.3
	Female	73	48.7
Age	18-21	26	17.3
	22-25	109	72.7
	25-29	15	10
Ethnicity	Malay	62	14.3
	Indian	9	6
	Chinese	69	46
	Others	10	6.7
Education	Undergraduate	107	71.3
	Postgraduate	43	28.7

The mean values of all the variables in this study, which range from 3.82 to 4.31, are shown in Table 2. Conversely, the dependent variable, self-protection had the highest mean score (4.31). Awareness (M=4.14) with a standard deviation of 0.94 came next. The social influence produced the third score, with a mean of 3.53 points and a standard deviation of 0.59 points. The social impact got the minimal mean score (M=2.47) with a standard deviation 1.05. The determinant variable of self-efficacy shows a mean score of 3.82. The results indicate a high score of consumers' self-protection and awareness. In contrast, self-efficacy and social influence were at a moderate level. The result shows that the respondents had high awareness and knew how to protect themselves, but at the same time, their self-efficacy level can be improved.

Table 2
Descriptive analysis of the variables

Variable	Mean Score	Standard Deviation
Self-efficacy	3.82	0.99
Social influence	3.53	1.05
Awareness	4.14	0.94
Self-protection	4.31	0.84

Note: Scale range 1-5

The results from multiple linear regression analysis are shown in Table 3, indicating the most important self-protection predictor. Using multiple regression analysis, the researchers evaluated the strength of the relationship between an outcome (the dependent variable) and several predictor variables and the significance of each predictor to the relationship. The first set of analyses examined the significant regression equation (F(71.961) = 13.936, *p* = .000) with an adjusted R^2 of .147. Only 14.7% of the model can explain the self-protection. The model is also found to be significant (p<0.01); thus, the $H_0 1$ is rejected. Among the three variables, self-efficacy (β=0.292; p=0.000) and awareness factor (β=0.551; p=0.000) were significant predictors of consumer self-protection. One can contend that awareness is the most significant determinant of an individual's motivation in online scam avoidance conduct (Baral & Arachchilage, 2019). The discovery is compatible with earlier studies that disclosed a positive correlation between self-efficacy and secure conduct to prevent Internet fraud (Daud et al., 2020; Nawi et al., 2023). It also supports the outcome of a previous study by Ridho (2024) and Burton et al. (2022) that states that awareness influences consumers' self-protection. However, this study's result is not aligned with the previous study by Wang, Zhu & Sun (2021) and Sharma et al. (2022), which states that social influence motivates consumers to protect themselves against scams.

Table 3
Purchase Decision Factors

Variables	Unstandardised Coefficients (B)	Standardised Coefficients Beta	T	Sig.
(Constant)	1.782		13.936	0.000
Self-efficacy	.292	.303	7.473	0.000*
Awareness	.551	.145	2.815	0.000*
Social influence	-.043	-.045	-.873	0.347

.R=0.325; R^2=0.337; Adjusted R^2= 0.147; F=71.961; Sig. F=.000; *p<0.01

Conclusion

This study was conducted to determine the factors that enhance consumers' self-protection against online scams. Three factors were proposed in this study's framework: self-efficacy, social influence and awareness. Based on the analysis test results, two factors have been proven significant and contribute to enhancing consumers' self-protection against online scams. The factors were self-efficacy and awareness. The findings indicate that awareness is critical to protect consumers against scammers. Awareness must be inculcated among consumers, and they will be able to share information and warnings regarding suspected scams involving online platforms that might alert other consumers in the surroundings.

Empowering discussions around scams is imperative to build consumers' self-efficacy and make them more resilient and able to protect themselves. Through consumer education, positive self-protection against online scams can be reinforced. Nevertheless, social influence is not a predictor, which shows that in Malaysia, peers, family, and friends will not influence them. This may be because the current anti-social behaviour adopted by consumers might perceive that social influence gives them neither a positive nor negative impact towards their lifestyle and decision-making (Halabi et al., 2024).

Implication of Study

The implications obtained through this research can be applied to several groups, such as consumers, government agencies, consumer movements, and industry players comprising financial services, internet merchants, and online platforms. Firstly, consumers should be prepared to face the upcoming challenges, especially in daily transactions. It is crucial to be extra cautious when purchasing online, and it is necessary to take preventive measures such as reviewing the seller's reputation before making any purchases online and being cautious of cheap deals that seem too good to be true. Self-defense is the best shield while surfing the Internet to avoid online scams. Consumers should not entirely depend on the Royal Malaysia Police (RMP) for constant protection against online scams all the time.

Furthermore, there are several implications for government agencies and consumer associations. NGOs and government agencies are essential in combating scams through consumer education. Their efforts to raise awareness and provide resources are critical in protecting consumers from fraudulent activities. By working together, they create a comprehensive approach to scam prevention that empowers consumers and helps maintain a safe and trustworthy marketplace. For example, educational materials should highlight the dangers of fake e-commerce sites and offer tips for verifying the authenticity of online sellers.

The industry, including the online marketplace, has also been crucial in promoting scam awareness and self-efficacy among consumers. By leveraging communication, transparency, technology, partnerships, and customer support, online businesses can significantly reduce the risk of scams. These efforts protect consumers and enhance trust and credibility in the marketplace, benefiting online businesses and their customers.

Furthermore, the findings from this study will contribute to the body of knowledge as they will serve as reference material or a guide for those who will embark on research in related fields of study. Since it is a quantitative method, the instruments can benefit other researchers who want to conduct consumer research.

References

Alzghoul, J. R., Abdallah, E. E., Al-khawaldeh, A. & Hafiz S. (2024). Fraud in online classified ads: Strategies, risks, and detection methods: A survey. *Journal of Applied Security Research, 19*(1), 45–69.

Andrei, F., & Veltri, G. A. (2024). Social influence in the darknet market: The impact of product descriptions on cocaine sales. *International Journal of Drug Policy, 124,* 104328.

Arimbawa, I. P. A. P., & Priyanto, I. M. D. (2024). Analysis of legal protection for online shopping consumers. *Policy, Law, Notary and Regulatory Issues, 3*(2), 222-227.

ASEAN (2018). Handbook on ASEAN consumer protection laws and regulations. ASEAN Secretariat, Jakarta.

Bandura, A. (1995). *Self-efficacy, adaptation, and adjustment: Theory, research, and application.* Springer US.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachandran (Ed.), *Encyclopedia of human behaviour*. Academic Press.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall, Inc.

Baral, G., & Arachchilage, N. A. G. (2019, May). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. *Proceedings of the 2019 Cybersecurity and Cyber Forensics Conference* (CCC), 102-110.

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems, 61(*3), 195-206.

Brenncke, M. (2024). A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations. *Journal of Consumer Policy, 47*(1), 127-164.

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology, 159,* 111678.

Chan, S., & Lu, M. (2004). Understanding internet banking adoption and use behavior: A Hong Kong perspective. *Journal of Global Information Management, 12* (3), 21–43.

Dangi, M. R. M., & Yacob, N. H. M. (2013). Examining the fraud awareness from the university's academic staffs perspectives. *Gading Journal for Social Sciences. 17*(02), 1-20.

Daud, N. A., Arif, A. M. M., Abu, E., & Bakar, S. O. (2020). Determinants of self-protection practices in online shopping among the students of higher education institutions, Malaysia. *Malaysian Journal of Consumer and Family Economics, 25*(1), 91-110.

Dol, N., Bakar, E. A., & Said, A. M. (2015). Consumer legal literacy, values and consumerism practices among members of consumer association in Malaysia. *Asian Social Science, 11*(12), 189-183.

Ellis, J. D., & Tucker, M. (2009). Factors influencing consumer perception of food hazards. *CABI Reviews,* 1-8.

Halabi, K. A., Shahrill, M., Roslan, R., & Adnan, M. (2024). The influence of impulsivity and anti-social behaviour on academic performance of university undergraduate students in Nigeria. *Jurnal Al-Sirat, 24*(1), 201-211.

Hanus, B., & Andy, W. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33* (1) 2–16.

Igbinenikaro, E., & Adewusi, A. O. (2024). Financial law: Policy frameworks for regulating fintech innovations: ensuring consumer protection while fostering innovation. *Finance & Accounting Research Journal, 6*(4), 515-530.

Johri, A. & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of Banking Digital Transformation. *Human Behavior and Emerging Technologies,* 1–10.

Luu, V., Land, L., & Chin, W. (2017). Safeguarding against romance scams–using protection motivation theory. *Proceedings of the 25th European Conference on Information Systems (ECIS),* 2429-2444.

Markus, H.R., & Kitayama, S. (1991). Cultural Variation in the Self-Concept. In J. Strauss, G.R Goethals (Eds.), *The self: Interdisciplinary approaches.* Springer.

Mariyappan, N., & Sangeetha, G. (2024). A study on consumer education towards external stimuli affecting online shopping behavior–analysis using Jamovi. *Educational Administration: Theory and Practice, 30*(4), 5985-5991.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92,* 139-150.

Modic, David and Modic, David and Lea, Stephen E. G. (September 10, 2012). How neurotic are scam victims, really? The big five and internet scams. https://ssrn.com/abstract=2448130 or http://dx.doi.org/10.2139/ssrn.2448130.

Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law and Society Review,* 467-496.

Nataraj-Hansen, S. (2024). More intelligent, less emotive and more greedy: Hierarchies of blame in online fraud. *International Journal of Law, Crime and Justice, 76*, 100652. –

Nawi, N. H. A., Mohamed, S., & Ramdzan, M. R. (2023). Understanding the Social Commerce Scam and Consumers Self Disclosure. *International Journal of Business and Technology Management, 5*(2), 251-262.

Rakin S. A., Md. Kais K. E, Sanjana F. A., & Durjoy, S. M. M. (2024). Security analysis in online transaction systems: a proposed framework. *International Journal of Information Engineering and Electronic Business (IJIEEB), 16*(2), 22–38.

Ridho, W. F. (2024). Unmasking online fake job group financial scams: A thematic examination of victim exploitation from perspective of financial behavior. *Journal of Financial Crime, 31*(3), 748-758.

Roscoe, J. T. (1975). *Fundamental research statistics for the behavioural sciences* (2nd ed.). Holt Rinehart & Winston.

Royal Malaysian Police (2022). https://www.rmp.gov.my/news-detail/2022/11/10/artikel-pilihan-scam-alert-tips-on-how-to-spot-online-scams-and-protect-your-digital-footprint.

Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economics Survey, 32*(5), 1292-1325.

Sarno, D. M., & Black, J. (2024). Who gets caught in the web of lies?: Understanding susceptibility to phishing emails, fake news headlines, and scam text messages. *Human Factors, 66*(6), 1742-1753

Sharma, S., Singh, G., Gaur, L., & Sharma, R. (2022). Does psychological distance and religiosity influence fraudulent customer behaviour? *International Journal of Consumer Studies, 46*(4), 1468-1487.

Statista. (2022). *E-commerce fraud - statistics & facts.* https://www.statista.com/topics/9240/e-commerce-fraud/#topicOverview

Statista. (2024). *Number of e-commerce scams in Malaysia 2021-2023.* https://www.statista.com/statistics/1346657/malaysia-number-of-e-commerce-scams/

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access, 9,* 11895-11910.

Wikström, P. O. H., & Kroneberg, C. (2022). Analytic criminology: Mechanisms and methods in the explanation of crime and its causes. *Annual Review of Criminology, 5,* 179-203.

Wong, A. T. T. (2019). A study of purchase intention on smartphones of post-90s in Hong Kong. *Asian Social Science, 15*(6), 78.

Wood, W. (2000). Attitude change: Persuasion and social influence. *Annual Review of Psychology, 51*(1), 539-570.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal, 30*(5), 791-844.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.