INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 12, (2023) E-ISSN: 2222-6990

Determinants of Fraud Victimizations in Malaysian E Commerce: A Conceptual Paper

Zulkifli Mohamad, Zurina Ismail, Ayu Kamareenna Abdullah Thani

Faculty of Business and Management, Universiti Teknologi MARA (UiTM), Malaysia

Corresponding Author Email: ayukamareenna@uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i12/20395 DOI:10.6007/IJARBSS/v13-i12/20395

Published Date: 23 December 2023

Abstract

Malaysia's eCommerce industry is constantly growing, fueled by COVID-19-related online services and the country's increasing smartphone usage Data.The World Health Organization declared the COVID-19 outbreak to be a global pandemic.On March 11, 2020, various countries responded quickly with tight social confinement enforcement (commonly referred to as "lockdowns") as an effective approach to regulate human interaction and viral transmission. With stay-at-home restrictions, travel bans, and social isolation, many people are joining the growing trend of internet purchase. Changes in customer behavior and government reactions have had an impact on the biological systems and economy of the cyber world. This study is expected to provide insights into the factors that impact cybercrime victims in Malaysian e-business. Similarly, prior research on fraud have primarily focused on traditional and offline fraud, with little data in the online or fraud victims arena. As a result, this study contributes fresh theoretical connections and empirical evidence on the interplay between fraud victimization, suitability and lack of a guardian. This study looks at the variables that affect Malaysian e-commerce fraud victimization, and it is anticipated that the study's population includes all of Malaysia in terms of cyberfraud. Individuals connected to cyber fraud will be the unit of analysis in this cross-sectional study, which uses a survey methodology. The PDRM database will be used to choose the study's respondents. A series of questionnaires will be used as the research instrument in this study to gather data, and respondents will get a set of questionnaires to complete.

Keyword: Fraud Victimization,Suitability And Lack Of A Guardian.

Introduction

E-Commerce (electronic commerce) refers to the online purchase and sale of productsand services. The exchange of goods and services between firms, persons, or entities is defined as the major root of the word "commerce." If you add an e to the beginning of the term,itsimply means the same thing when done on the internet. Electronic commerce (ecommerce)isa business strategy that allows consumers and businesses to buy and sell goods and servicesover

the Internet. Ecommerce can be done on computers, tablets, smartphones, and other smart devices, and it operates in four key market categories. It is impossible to overestimate the impact of ecommerce on retail(Azizah, 2021).

Global ecommerce sales are anticipated to reach $6.3 trillion in 2023. This representsa 10.4% growth over the previous year, as the global ecommerce market continues to expandyear after year (Lee et al., 2023). According to a recent assessment of ecommerce market sizeby country, China is predicted to be the world's largest ecommerce market in 2023. Malaysia's ecommerce market is rapidly growing to become one of the largest in Southeast Asia. Its expansion is exceeding that of the region's typical established markets.

The Malaysian e-commerce market has been registering growth during the last few years, which has been further accelerated by the COVID-19 pandemic. This, coupled with thegrowing consumer preference for online shopping, availability of customized online payment options, and government support, will further drive the e-commerce market in Malaysia (Shah, 2020).

The Department of Statistics Malaysia is now sharing statistics and data related to Malaysia's demographics for the first quarter of 2023, showing that the totalpopulation in Malaysia has now reached 33.2 million people. This also shows a population growth of 1.6% compared to the same period last year. According to Judget et al. (2017) there were 32.03 million internet users in Malaysia at the start of 2023, when internet penetration stood at 96.8 percent.

It's only logical that as ecommerce grows, so will the number of online shoppers worldwide. As of 2023, the total number of digital buyers is 2.64 billion. This accounts for 33.3% of the global population. To put it another way, one out of every three persons you see is an internet shopper. The number of online shoppers has been growing over the past few years. In2023, there are 80 million more digital buyers than there were in 2022—a 3.1% year-over-year increase (Tajpur & Zamani, 2020).

In battling Covid-19 pandemic, scammers have bilked Americans out of $545 million infraud since the beginning of 2020 in a range of schemes from online shopping to travel, according to the Federal Trade Commision (FTC). The agency received almost 589,000 consumer complains associated with the pandemic from Jan. 1, 2020, to Aug. 30, 2021. Roughly 61% of the report concerned fraud; the median loss was $380. Online shopping accounted for the largest number of reported scams to the FTC, at nearly 55,000 complaints.Victims lost the largest amount of total money ($79 million) to vacation and travel scams, according to FTC data. The Federal Trade Commission’s (FTC) Consumer Sentinel Network took in over 5.1 million reports in 2022, of which 46 percent were for fraud and 21 percent for identity theft. Credit card fraud accounted for 43.7 percent of identify thefts, followed by miscellaneous identity theft at 28.1 percent, which includes online shopping and payment account fraud, email and social media fraud, and other identity theft .

Director of JSJK Bukit Aman, Datuk Zainuddin Yaacob, (2021) said the number of arrests involving e-commerce criminals also increased sharply in 2020 involving 2,250 individuals compared to 1,397 arrests in 2019 (Shah, 2020). From the increase in statisticsas reported, it can be stated that there are a handful of youths who are behaving in deviant behaviour using the medium of online business to reap profits and self-interest without thinkingof other users. This behaviour also causes losses to the economy of the country as well as losses to users of online businesses. The seriousness of cyber-crime in nature to involve lossof money and property has been causing several acts to be enacted in Malaysia aimed at curbing the treatment of such crimes (Maskun, 2014).

This is proven by the statistics of the investigation paper of the Commercial Crime Investigation Department for the year 2017 to 2021. From the statistics (2022), it is stated that e-commerce crime cases involve media platforms such as Facebook, Mudah.my, Carousell, WhatsApp, Instagram, Social Web, E-Bay, E-mail, and WeChat. The number of cases and annual total lost presented in table 1.1 an

Table 1.2.1:
E-Commerce Crime Cases Platform

e-commerce crime cases platform	2017	2018	2019	2020	2021	2022
Facebook	1,249	777	1016	2305	4033	3341
Mudah.my	2,954	1186	1061	1072	749	134
Corousell	162	168	144	138	145	72
Whatsapp	306	217	265	504	903	2514
Instagram	278	347	517	1060	2429	1054
Social Web cases	31	46	17	38	61	276
e-bay	11	5	2	0	3	6
Email	30	14	6	13	18	8
Wechat	56	107	103	92	52	43
Total cases	5,077	2,867	3,131	5,222	8,393	9,470

Table 1.2.2:
Total lost annually

Year	2017	2018	2019	2020	2021
Total lost (RM)	20,629,164.00	16,563,263.43	16,808,757.51	34,209,710.94	61,094,059.26

Year	2022
Total lost (RM)	112,717,995.51

In the data of this study, the highest state cases in e-commerce fraud are the State of Selangor, followed by the States of Johor, Perak, Negeri Sembilan, Melaka and Kuala Lumpur. Based on a report received by the Ministry of Trade and Consumer Affairs (KPDNHEP),2019 recorded the most cases of online fraud (Muhammad Afham 2019). State KPDNHEP Chief Enforcement Officer, Azman Adam detailing that a total of 110 complaints were receivedin less than two months. Meanwhile, in less than two years, PPIM received more than 30,000 complaints fraud (Bashir et al., 2021). These statistics show an increase in fraudcomplaints among online shoppers is increasingly alarming. The number of losses suffered by consumers due to fraud is also estimated to reach thousands to millions ofringgits for a singlecase (Ismail et al., 2023). The total loss suffered by consumers is RM410 million involving 8,489 fraud cases (Shah, 2020).

This study is forecast to provide insights into factors that influence the victims of cybercrime in Malaysian e-business. Similarly, previous studies on fraud mostly focused on traditional and offline fraud, and in terms of the online or fraud victimization field is still lacking evidence. Therefore, this study adds new theoretical linkages and empirical evidence on the interaction between suitabilityand lack of guardian towards fraud victimization.

Literature Review

Fraud victimization

The notion that fraud victims are risk takers who may sometimes share responsibility for their victimization is a widespread cultural trope. It is encapsulated in adages like "you can't cheat an honest man" and "there's a sucker born every minute." These words imply that both the perpetrator and the victim of fraud engage in risky business, and that bad luck may not be the primary cause in fraud victimization. Fraud is defined as committing misleading or dishonest acts for personal advantage, usually financial gain, by misrepresenting oneself or promising things, services, or financial benefits that do not exist, were never intended to be supplied, or were misrepresented (Zhang & Ye, 2022). In general, fraud victimization is a type of economic crime. This category may cover a range of crimes, but fraud victimization often takes one of two forms: victimization of organizations or victimization of individuals. There is substantial evidence that fraud victimization is increasing, and that losses suffered by victims of fraud far outnumber those suffered by victims of street crime. Given that many fraud victims are hesitant to report their victimization to law enforcement; the situation is likely to be worse than official figures indicate. Fraud happens in all modes of communication, including face-to-face conversations, phone calls, text messages, and, increasingly, the internet and related social media platforms. According to Kemp et al. (2023), "online fraud"

is "the experience of a person who has responded through the use of the internet to a dishonest invitation, request, notification, or offer by providing personal information or money, which has resulted in the suffering of a financial or non-financialloss of some kind."

Suitability

Target suitability refers to being vulnerable or open to perpetrators' actions (Kenny & Kenny, 2020). The offender's impression of the target's vulnerability influences the choiceof suitable targets; the more suitable and accessible the target, the more probable a crime willoccur. A suitable target must converge with a motivated offender at the same time and place for a crime to occur, which means that both the target and the offender must engage in similar routine activities for the convergence to occur (Smith & Stamatakis, 2020).

An appropriate suitable target is a person that an offender may threaten. Felson favours the term "target" to "victim" since the former emphasises that the majority of crimes are committed to gain things, and so the "victim" may be gone from the scene of the crime (Ghazi & Pontell, 2022). The term "suitable target" is still a bit of a misnomer, and different definitions have been proposed in the past. Even yet, one of the simplest approaches of determining what constitutes an "appropriate target" is to evaluate any person or item who is likely to be seized or attacked by the offender (Maimon et al., 2019). Target suitability has since been applied to many more types of crimes, for example, drug dealing, cybercrime, and white-collar crime.

Lack of guardianship

According to Wacsh et al. (2021), guardianship is carried out by people or system who act"by simple presence to prevent crime and by absence to make crime more likely." When thereis a higher chance of detection and subsequent punishment or censure for undesirable behaviours as a result of a perception that someone who could notice and notice inappropriate behaviours is watching, guardianship can operate. In accordance with Payne (2020), "the prime guardians in society are people whose presence, proximity, and absence make it harder or easier to carry out criminal acts"

The lack of a guardian capable of preventing a threat increases thelikelihood of becoming a victim of crime. Guardianship is described as "the physical or symbolicpresence of an individual (or group of individuals) that acts (either intentionally or accidentally)to avert a possible criminal event" (Payne, 2020). Guardianship can take the shape of a person physically present who can act as a protector, or it might take the form of more passivemechanical technologies like video surveillance or security systems. These physical security measures aid in restricting an offender's access to appropriate targets.

Research design

This study will apply quantitative method. This is because quantitative is based on testing theory, observation, survey, and analysis of the data through distribution of questionnaires. According to Sekaran and Bougie (2016), various aspects of research design are involved such as the purposed of study, research strategy, unit of analysis, and time horizon. In this study, the quantitative research method is used to present numerical data that can be used totransform the researcher's statistics. According to Sekaran and Bougie (2016), a research design is a blueprint or plan for collecting, measuring, and analyzing data in order to answer the research questions that have been developed in one particular study.

Sampling Design

Sampling design is a sample design attributes through plan and method to be followed by selecting a sample from the targeted population and estimation technique formula for computing the sample statistic (Al Majd, 2020). The fundamental element of the research was a review of factors that affecting fraud victimization among online users in Malaysia. This research aims to determine the factors that affecting fraud victimization. Data regarding exposure, suitability, lack of guardianship is what leads to the fraud victimization through literature review.

Population

Data collection for this survey is start with numbers e- Commerce users in Malaysia. Malaysia's eCommerce market has never been stronger than in 2023. With growing internet penetration, and smarter, more powerful devices, consumers are increasingly flocking to buy products and services online. Based on the Ministry of Communications and Digital until September 2023, Malaysia recorded 28 million social media users or 86 percent of the country's population. According to Statista Research Department the number of users in the E-commerce market in Malaysia reach to 16.71 million in 2023.

Conclusion

As a conclusion, this study examines the factors that influence the fraud victimization in Malaysian e- business and the population of this study is expected to cover the whole Malaysia in term of cyber fraud. Current study is a cross-sectional study using survey method and individual whorelated to cyber fraud will be the unit of analysis. The respondents of this study will be selectedt hrough the PDRM database. This study expected to use a set of the questionnaire as the research instrument to collect the data and the respondents will be given a set of questionnaires to answer.

References

Al-Majd Mohamad, O. A. (2022). Islamic Literature Examining Food Fraud Regulations from A Systematic Review Approach. American J Sci Edu Re: AJSER-101.

Azizah, S. N. (2021). Cyber-Crime and Fraud Victimization of Online Halal Meat Shops: A Negative Image Propagation. International Journal of Cyber Criminology, 15(1), 158-173.

Bashir, S., Khwaja, M. G., Mahmood, A., Turi, J. A., & Latif, K. F. (2021). Refining e-shoppers' perceived risks: Development and validation of new measurement scale. Journal of Retailing and Consumer Services, 58, 102285.

Ismail, A. S., Haniff, M. A. M. M., & Md, M. N. (2023). Inside the Mind of Cybercriminals: Investigating the Influence of Socioeconomic Factors on the Ethical Decision-Making of Cybercriminals. In Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023 (p. 34).

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. 2017. The role of cognition, personality, and trust in fraud victimization in older adults. Frontiers in psychology. 8: 588.

Kenny, J. F., & Kenny, J. F. (2020). "Getting to Know You": Confirming Target Suitability. Hiding in Plain Sight: Deceptive Tactics and the Criminal Victimization Process, 59-69.

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2022). Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. The Journal of Adult Protection, 24(3/4), 179-194.

Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. *Journal of Crime and Justice*, *42*(5), 516-535.

Payne, B. K. (2020). Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice*, *45*, 563-577.

Shah, A. (2020). A Study of Online Scams: Examining the Behavior and Motivation Factors of Scammers and Victimization Consequences. In *Leveraging Consumer Behavior and Psychology in the Digital Economy* (pp. 81-90). IGI Global.

Smith, T., & Stamatakis, N. (2021). Cyber-victimization trends in trinidad & tobago: the results of an empirical research. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(1), 46-63.

Tajpour, A., & Zamani, M. (2020). Identity Theft and Prevention. *Information Security and Optimization*, 25-42.

Wachs, S., Mazzone, A., Milosevic, T., Wright, M. F., Blaya, C., Gámez-Guadix, M., & Norman, J. O. H. (2021). Online correlates of cyberhate involvement among young people from ten European countries: An application of the Routine Activity and Problem Behaviour Theory. *Computers in Human Behavior*, *123*, 106872.

Zhang, Z., & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. *Frontiers in Psychology*, *13*, 1030670.