INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ECONOMICS & MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 13, Issue 2, (2024) E-ISSN: 2226-3624

Applying Routine Activity Theory to Determine What Exposes Malaysian E-Commerce Fraud Victims

Zulkifli Mohamad, Zurina Ismail & Ayu Kamareenna Abdullah Thani

Universiti Teknologi MARA Cawangan Kelantan

To Link this Article: http://dx.doi.org/10.6007/IJAREMS/v13-i2/19039 DOI:10.6007/IJAREMS/v13-i2/19039

Published Online: 03 April 2024

Abstract

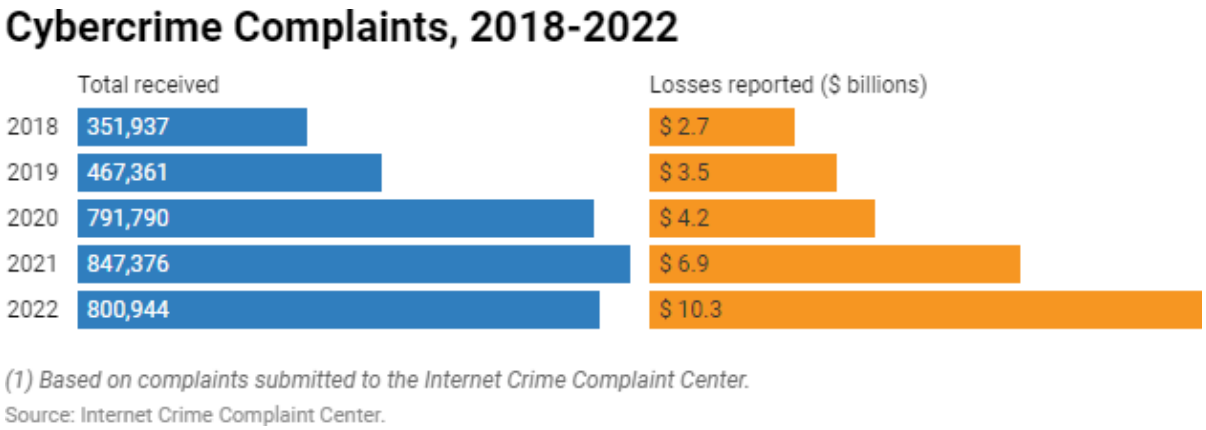
The internet's creation and growth created a new virtual world that was very similar to our real world. This created many great chances for people to make their lives better. The internet lets people stay in touch in real time over long distances for little money. One more thing you can do from home is shop, work, or study. Thanks to online identification systems, you can even do official administrative tasks linked to citizen issues. On the other hand, big and quick changes in technology make it easier for both good people and businesses to adapt to these new technologies and for bad people to change how they do things quickly. The Routine Activity Theory is a great way to look into online abuse because it is a key theory on the subject. The Routine Activity Theory is the main idea behind this study. Because of the small size of this study, this paper will only look at how psychological traits affect the chance of becoming a victim of fraud and how exposure to fraud affects becoming a victim of E-Commerce fraud.

Keywords: Routine Activity Theory, Exposure to E- Commerce, Fraud Victimization, Personality Traits.

Introduction

According to the FBI's Internet Crime Report 2022, criminals and enemies have many options to harm the United States thanks to the current cyber landscape. Global cyber dangers are present, and humans have seen an increase in the size and complexity of these schemes and attacks and also report 2022, 800,944 complaints of cyber- crime were reported to the FBI by the public, a 5 percent decrease from 2021. However, the potential total loss increased to $10.2 billion in 2022, up from $6.9billion in 2021. California, Florida and Texas had the highest number of cybercrime victims, refer the table below:

Table No: 01



(1) Based on complaints submitted to the Internet Crime Complaint Center.

Source: Internet Crime Complaint Center.

The Federal Trade Commissions (FTC) report that since the start of 2020, con artists have defrauded Americans out of $545 million in fraud as part of its efforts to combat the Covid-19 pandemic. The schemes vary from online shopping to vacation. Between January 1, 2020, and August 30, 2021, the government received approximately 589,000 consumer complaints related to the epidemic. The report focused mostly on fraud, with a median loss of $380. With almost 55,000 complaints, online shopping accounted for the greatest number of frauds submitted to the FTC. According to FTC data, victims lost the most money overall ($79 million) as a result of vacation and travel scams. In 2022, the Consumer Sentinel Network of the Federal Trade Commission (FTC) received over 5.1 million reports, of which 21% and 46% were related to identity theft and fraud, respectively. 43.7 percent of identity thefts were related to credit card fraud, with miscellaneous identity theft (which includes email and social media fraud, online shopping and payment account fraud, and other identity theft) coming in second at 28.1 percent (Abidin et al., 2019). In 2021, victims of online purchase fraud or trade fraud reported multiple incidents (or methods of operation) to the Royal Malaysian Police (RMP).
Examples of cases are as follows:

Case 1: On December 18, 2021, around 1605hrs, the victim was tricked while browsing the Facebook Group, Vegetable, Fish, Fruit, and Retail Wholesaler ID. The victim had been in touch with the suspect through the WhatsApp line provided. In the transaction, the victim was offered a price of RM42.60 per box of cooking oil. The victim agreed to the price offered and wanted to buy as many as 200 boxes. The suspect had instructed the victim to deposit money into a bank account provided by the suspect. The victim had made a payment transaction to an account that had been given RM6,191.00 and had been deceived in the purchase (Commercial Crime Investigation Department, 2021).

Case 2: The victim was a Malay woman who was deceived on December 30, 2021. The victim was deceived while browsing Instagram under the name "Maccity Apple store" to buy an iPhone 11worth RM350.00. The victim then communicates with the suspect through the WhatsApp app on the given line. The victim agreed to the price of the advertisement, but the victim did not realise that he had been tricked into making money transactions into the account given by the suspect up to RM5,350.00 (Commercial Crime Investigation Department, 2021).

Case 3: The victim, a Malay man, was deceived on October 23, 2021, while browsing the mudah.my application. The victim was attracted by an advertisement for the sale of a Backhoe 580 K vehicle with a price of RM28,000.00. The victim contacted the seller through the telephone number provided and made an advance payment of RM7,000.00 to the bank account provided by the suspect as instructed by the online seller. After payment is made, the victim tries to contact the seller but is unsuccessful (Department of Commercial Crime Investigation, 2021).

Reacting to the arising cases, the Online Commercial Crime Prevention Campaign is further strengthened by making it an annual event in an effort to create public awareness of the modus operandi of online fraud syndicates. In order to mitigate the fraudulent activities in online purchases, the PDRM, especially the Commercial Crime Investigation Department (JSJK), has held awareness campaigns at the Bukit Aman level and also at the contingent level (JSJK, 2022). According to the campaign data collected by JSJK in 2022, prevention campaigns were implemented through exhibitions, lectures, and media broadcasts all around Malaysia. Despite the commercial crime prevention campaign executed for the past 3 consecutive years, online fraud cases still recorded an increasing trend. E-commerce fraud is a serious crime and fraudulent activities in online business have still become a major concern for the authority and more stringent action needs to be strategized. However, prior to that, understanding on the causes that contributed to the consistent rise in e-commerce fraud cases. Prior studies have also shown that victims of internet exploitation experience serious emotional and psychological repercussions as a result of their victimizations. The most prevalent were loneliness, shame or humiliation, discomfort, despair, fury, worry, and shock.

Furthermore, Anuar et al (2023) notes that victims of online fraud experience long-term effects that affect their conduct. Their study shows that 74.5 percent of people who experience online fraud modify their conduct and become more watchful, nervous, and skeptical of others. Additionally, as a result of their online fraud experience, victims of online fraud may develop a number of physical ailments and negative health effects, such as insomnia, nausea, and weight loss. According to the Routine Activity Theory developed by Cohen and Felson (1979), criminal opportunities exist when the circumstances are favorable for the perpetrator to perform the criminal activities and the occurrence is contributed by three elements that is the offender, the target and the guardian. The routine activity theory is commonly used to explain the conventional crime activities, but this present study aims to applies the theory into the e- commerce crime setting and examine whether similar elements also cause the millennial (e- commerce) crime to occur. On other note, individual personality could also play an important role in causing the fraud to occur (Ahmad et al., 2020). Thus, this study argues that certain personality traits could possibly make the occurrence of fraud more appealing.

Research Objective

i. To test the impact of exposure on E- Commerce fraud victimization.

ii. To examine the role of personality traits in moderating the possibility of fraud victimization.

Significant of Study: In a real sense, this study should help people, businesses, and society learn more about the different factors that lead to cyber fraud. This worries me a lot because in Malaysian e-business, publicity and personality is one of the most important functional

areas and important points that will affect fraud. It is also expected that this study will help the government and the Royal Malaysian Police (RMP) make strong rules and laws to cut down on and get rid of cybercrime linked to e-business in Malaysia.

Limitation of Study: This study is a cross-sectional study, which means that the opinions about exposure and personality are gathered at a single point in time. Conditions and effects can change over time. It doesn't let you change the way you figure out cause and effect or how the result changes over time. Nawi et al (2023) say that a longitudinal study design could be changed to help researchers fully understand the cause-and-effect links between the factors. So, more research might focus on following this general cause-and-effect chain over time to get more detailed results. It is also helpful to know how exposure, suitability, lack of a guardian, and personality change over time. Comparative studies of the same cause model could also be done between developing and developed countries.

Literature Review

Fraud is the act of engaging in deceptive or dishonest behavior for personal benefit, typically involving financial gain. This is done by misrepresenting oneself or making false promises regarding non- existent or misrepresented items, services, or financial advantages (Ramoo et al., 2023). Fraudulence occurs across various communication channels, encompassing in-person dialogues, telephone chats, text- based exchanges, and, notably, the internet and its associated social media platforms. According to Cross (2016), "online fraud" is when someone reacts to a fake online invitation, request, notification, or offer by giving away personal information or money, which results in a loss of money or something else of value.Although criminals have countless strategies at their disposal to target individuals, there are distinct categories that they commonly utilize. Advance fee fraud (AFF) and phishing exemplify these phenomena. Advance fee fraud (AFF) is a type of scam where victims are solicited for a small sum of money in exchange for the promise of a bigger sum in the future. AFF approaches are utilized in investment programs, inheritance announcements, lottery win notifications, employment schemes, and charitable activities (Rasheed et al., 2023). Phishing strategies aim to get personal information from individuals by impersonating a reputable organization, typically through email or text messages. The sender asks the recipient to provide personal information, such as banking details, passwords, and other sensitive information (Chen et al., 2021). Once the victim responds, the criminals employ the provided credentials to gain unauthorized access to bank accounts and credit cards, so engaging in identity fraud.

The Related Theory (Routine Activity Theory): Criminology has done a lot of study on Routine Activity Theory in the real world, but researchers aren't sure how well it works in cyberspace (Singh et al., 2021). It wasn't hard to show that the internet is full of bad people with bad intentions, like hackers, stalkers, and scammers. People who are good targets share personal information, make purchases, or use online funds. Administrators, users, and friends are all good internet guardians, but so is technology like firewalls, antivirus software, and private networks (Yeasmin & Wu, 2021). Routine Activity Theory gives us a way to look at the traits of a victim in order to understand how victims are hurt in cyberspace (Zhon & Asiama, 2022). When people do these normal things, they are often around likely offenders, or people who have the means and the desire to commit physical or financial crimes. When strong guardians

aren't around, like police officers or private security guards, these weak people are more likely to be targeted by criminals (Utami, 2021).

Additionally, even whether they are physically, socially, or virtually near to the offenders, not everyone has the same risk of being a victim. Some people are more suitable targets for criminals and hence more vulnerable to victimisation due to certain demographic, psychological, economic, social, and behavioural traits (Yong et al., 2023).

Exposure/ The Presence of a Motivated Offender: One of the major parts of RAT is exposure to offenders, which is defined as "the physical visibility and accessibility of persons or objects to potential offenders" (Rosario, 2022). Traditional crime studies have revealed that engaging in activities outside of the home increased exposure/proximity to motivated offenders, hence raising the likelihood of victimisation (Tillyeret al., 2011). Based on its accessibility, a target is chosen by the perpetrator. In contrast, proximity in cyber space is different. When a crime is committed online, the victim and the perpetrator do not have to be there at the same time. According to Tharshini et al (2022), everyone is merely a click away from the internet. According to Mauritius et al (2020) motivated offenders are challenging to stay away from because they operate in the same neighborhoods online. The Internet has a high crime rate, and criminals are constantly hunting for a good target. Motivated criminals have chances thanks to how technology works. In the world of internet, the physical distance between the victim and the criminal is irrelevant. In the real world, criminals search for a suitable location to attack a victim, but the entire internet is a good option for them. A target can be attacked by the perpetrator from great distances. Tools are available on the internet itself that facilitate an attacker's attack on a target. They choose a victim based on their regular internet behaviors.

Exposure/ The Presence of a Motivated Offender: As Cohen et al (1981) say, "exposure to offenders" means "the physical visibility and accessibility of persons or objects to potential offenders." This is a big part of RAT. Traditional crime studies have shown that doing things outside of home makes you more likely to be targeted by criminals, which increases your chances of becoming a victim (Tillyeret al., 2011). The criminal picks a target based on how easy it is to get to. Cyberspace closeness, on the other hand, is not the same. When a crime is committed online, the victim and the perpetrator do not have to be there at the same time. According to Azizah (2021), everyone is merely a click away from the internet. According to Chen et al (2021) Motivated offenders are challenging to stay away from because they operate in the same neighborhoods online. The Internet has a high crime rate, and criminals are constantly hunting for a good target. Motivated criminals have chances thanks to how technology works. In the world of internet, the physical distance between the victim and the criminal is irrelevant. In the real world, criminals search for a suitable location to attack a victim, but the entire internet is a good option for them. A target can be attacked by the perpetrator from great distances. Tools are available on the internet itself that facilitate an attacker's attack on a target. They choose a victim based on their regular internet behaviour.

Personality trait as the Moderator: This study also looks at psychological trait as a moderator in understanding the link between exposure, suitability, lack of guardian, and fraud victimization. As Hayes (2013) says, a mediator is a qualitative or quantitative variable that changes the direction and/or strength of the relationship between an independent variable (also called a predictor variable) and a dependent variable (also called a criterion variable).

From reading other research, it has been suggested that personality may change the link between three types of independent factors and falling victim to fraud. Furthermore, this study finds that there is a need to support the relationship between the personality trait and the predictor variables mentioned earlier, as well as the relationship between the personality trait and the criterion variable, which is being a fraud victim. As a moderating variable, personality has never been fully measured in relation to being a victim of scam. Some people think that agreeableness, which is the tendency to get along with others Chen et al (2023), might have something to do with how easy it is to be tricked and scammed (Abidin et al., 2019). Being honest may also be linked to being a target of fraud, as shown by the honesty-humility personality trait as a moderating variable (Ghani et al., 2021).

Nawi et al (2023) research has shown that adults and kids who are honest tend to expect others to be honest as well. Finally, research on conscientiousness may show results that are similar to those found on executive functioning. Anuar et al (2023) say that being careful to think about the results of one action and paying attention to details are signs of being conscientious. Good people like to plan ahead instead of acting on the spur of the moment. People who are losing their executive functioning may find it hard to do these things, and people who are already lacking in this personality trait may be more likely to fall for fraud scams. Loka nan and Liu (2021) say that it is highly suggested that moderating variables are needed to explain how the predictor variable affects the criterion variable when trying to figure out what causes people to become victims of fraud. In their 2021 study, Singh et al. stated that fraud victimization can be relevant if a moderator is used to explain and understand how it is related to the predictors.

This is specifically parallel to the assertions by Yong et al (2023) that moderators could have the ability in explaining why and how a predictor influences an outcome variable which makes research result meaningful.

Research Framework

Various iterations of this theoretical framework are employed in the investigation of cybercrime using opportunity theory. Some research on cybercrime persecution has used RAT as its theoretical framework Anuar et al (2023), whereas other research has not (Ghani et al., 2021).

In this study, the research model involves an important variable including Independent Variable (IV) and Dependent Variable (DV). DV can be considered as the main issue in an attempt to examine, whereby, the IV is the element that attempts to influence the DV. In this study, exposure is referring to IV, personality as a moderator and fraud victimization refer to the DV.

Conclusion

Cybercrime is on the rise at a worrisome rate, and it hurts the people who are victims. Routine Activity Theory (RAT) is often used to figure out what makes people victims of hacking. Currently, RAT has seen the most support as a possible explanation for cybercrime.

References

Abidin, M. A. Z., Nawawi, A. & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*, 27(1), 81-100.

Ahmad, A. H., Masri, R., Zeh, C. M., Shamsudin, M. F. & Fauzi, R. U. A. (2020). The impact of digitalization on occupational fraud opportunity in telecommunication industry: a strategic review. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(9), 1308-1326.

Anuar, A., Ravintharan, D., Rosli, M. A. H., & Xuan, N. C. (2023). Factor influencing the intention to use E- Commerce among generation-y in Kota Bharu (Doctoral dissertation, Universiti Malaysia Kelantan).

Ansari, S. (2020). FROM THE SCAMMER PERSPECTIVE: PREDISPOSITIONS TOWARDS ONLINE FRAUD MOTIVATION AND RATIONALIZATION (Doctoral dissertation, Purdue University Graduate School).

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.

Chen, L. Y., Saw, J. W. R., Ding, K. Z. W. & Lean, R. Y. (2023). Online fraud: Factors affecting consumers' online purchasing behaviour in Malaysia (Doctoral dissertation, UTAR).

Chen, S., Yuan, Y., Luo, X. R., Jian, J., & Wang, Y. (2021). Discovering group-based transnational cyber fraud active: A poly methodological view. *Computers & Security*, 104, 102217.

Ghani, A. S. A., Wahab, H. A., Ghazali, A. S., & Azam, S. B. M. (2021). Contextual and multifactorial influence

on perception of safety from crime among selected Malaysians. *International Journal of Research in Business and Social Science (2147-4478)*, 10(8), 284-297.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 Pandemic. *International Journal of Information Engineering & Electronic Business,* 13(2).

Lokanan, M., & Liu, S. (2021). Predicting fraud victimization using classical machine learning. *Entropy*, 23(3), 300.

Mauritsius, T., Alatas, S., Binsar, F., Jayadi, R., & Legowo, N. (2020). Promo abuse modeling in e-commerce using machine learning approach. In 2020 8th International Conference on Orange Technology (ICOT) (pp. 1-6). IEEE.

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.

Ramoo, T. B., Sharif, M. S. M., Shariff, N. S. M., & Rahin, W. N. F. N. W. (2023). The effect of scammers on customer perception toward E-Commerce platform among Universiti Malaysia Kelantan students (Doctoral dissertation, Universiti Malaysia Kelantan).

Rasheed, F., Said, J., & Khan, N. I. (2023). EVOLUTION OF FRAUD-RELATED THEORIES: A THEORETICAL REVIEW. *Journal of Nusantara Studies (JONUS)*, 8(3), 322-350.

Rosario-Tavarez, C. (2022). Strategies Business Leaders Use to Mitigate Online Credit Card Fraud (Doctoral dissertation, Walden University).

Singh, M. M., Frank, R., & Zainon, W. M. N. W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, 10(3), 1658-1668.

Tharshini, N. K., Mas' ud, F. H., & Hassan, Z. (2022). Level of Cybercrime Threat During the Outbreak of COVID-19 Pandemic: A Study in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 12(5), 40-51.

Utami, M. S. M. (2021). The upshot of cybercrime and brand trust on customer purchase intention of e- commerce. *REVIEW OF MANAGEMENT, ACCOUNTING, AND BUSINESS STUDIES*, 2(2), 148-160.

Yeasmin, F., & Wu, X. (2021). Determinants of Cybercrime and its Impact on e-Commerce Development in Bangladesh. *Journal of Management and Humanity Research*, 6, 19-45.

Yong, H. N. A., Kuah, Y. C., Wei, C. Y., & Rafay, A. (2023). Consumer Risk Perception Towards Cybercrimes and E-Commerce: The Case of Malaysia. In Theory and Practice of Illegitimate Finance, 184-202). IGI Global.

Zhon, H., & Asiama, A. A. (2022). The Prevalence and Mechanisms of cyber fraud activities among