PREVALENCE OF ONLINE BUYING SCAM AND FRAUD EXPOSURE AMONG THE BUSINESS ADMINISTRATION STUDENTS

Gisela Kate Dae A. Ignes[1], and Ramonchito M. Nalangan[2]

[1]Student of the College of Business Administration Education, University of Mindanao, Bolton Street, Davao City, 8000, Philippines

[2]Faculty of the College of Business Administration Education, University of Mindanao, Bolton Street, Davao City, 8000, Philippines

ABSTRACT

This study determines the prevalence of online buying scams and fraud exposure among students. Respondents are one hundred seventy-five students from seven College of Business Administration Education proof the University of Mindanao enrolled in A.Y. 2022-2023. The adopted and modified questionnaire was utilized. Respondents are chosen using a purposive sampling technique. Frequency, percentage, average, Mann-Whitney U, and Wilcoxon W are the tools employed. The result shows no significant difference in respondents' exposure to the prevalence of online buying scams and fraud in terms of age, sex, year level, program, lifestyle, and routine activities. Hence, it is concluded that students are exposed to online buying scams and fraud regardless of their profile, lifestyle, and routine activities as long as they patronize online products. Thus, it is recommended that students should be careful with information and products offered online and should refrain from responding to unknown sources or good deals online. Buy from a reliable source/s or in the actual display, and not permit themselves to be influenced by social media endorsers since not all products and messages posted are legitimate and trustworthy. Also, it is recommended that the lawmaking body pass a law that would strongly regulate and penalize online scammers who employ fraud and victimize the innocent. Online sellers should have a license. Implementation and penalties should be stricter and heavier. Academe should make an information campaign among students on do's and don'ts in dealing online. Future researchers may investigate other aspects not covered by this study.

Keywords: *Prevalence, Online Buying, Scam, Fraud, Lifestyle, and RoutineActivities*

INTRODUCTION

Most people today engage with one another via Internet platforms, which have become indispensable. Online platforms provide the general public with a wide range of services and information, some of which may be real. This includes internet sales, where merchants frequently make unwarranted claims about their goods' purpose, benefits, and other aspects to persuade innocent buyers to purchase. They even employ various schemes and devices to reach their target market or target victims of scams and fraud (Daroch et. al., 2021). With the help of a deceptive website or a bogus ad on a legitimate shopping site, scammers pose as legitimate

internet vendors to defraud consumers. They often advertise luxury goods like famous brands of clothing and devices at meager prices, but you will receive a fake version of what you paid for or nothing. They attract online shoppers using refined designs, layouts, potentially stolen icons, logos, and domain names (PNP Anti-Cybercrime Group, 2022). Some might be unsuspecting victims of fraudulent transactions, unaware of the proper channels when reporting such an incident, or think it is not worth the effort (Ipsos, 2020). With the existing problem, the researcher is encouraged to study scam and fraud from the consumer viewpoint. It seeks to understand the effects of online buying scam and fraud exposure among business administration students and address the problem.The study helps broaden the knowledge of how social media may be a venue for scam and fraud.

This study is anchored to the Routine Activity Theory, which suggests that offenders choose whether or not to execute a crime depending on their access to the ideal target or the presence or absence of a competent guardian, as it may bring consequences on offenders (Nickerson, 2022). Correspondingly, crime rates depend on the population's constantly changing lifestyle and routine activity.

As shown in Figure 1, the main variable of this study is the prevalence of online buying scam and fraud exposure among the business administration students with indicators of lifestyle and routine activity. This study's moderating variable is the respondents profile, such as the age, sex, year level and program.

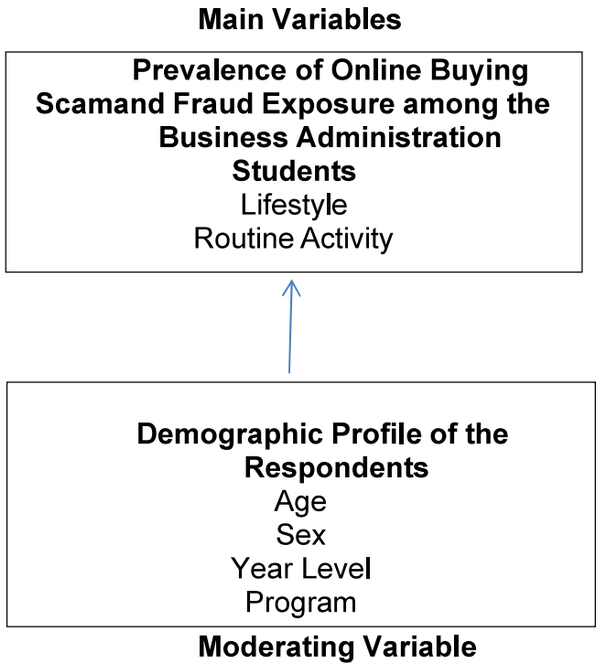

Figure 1. Conceptual Framework of the study

The study's objective is to determine and present the respondents' online buying scam and fraud exposure with its determinants: lifestyle and routine activity, when analyzed according to students' profile.

METHOD

The respondents of the study are a total of 175 students, of which 25 are taken from each of the seven programs from the College of Business Administration

Education of the University of Mindanao, Bolton, Davao City, officially enrolled in A.Y. 2022-2023. The purposive sampling technique and descriptive research design are used in selecting individuals and sites intentionally to determine the level of online buying scams and fraud exposure among business administration students. Data are analyzed using frequency, the percentage for profiles, and the average is used in determining the prevalence of online buying scams and fraud exposure level among students. The Mann-Whitney U-Test was used to compare the statistical scale of the prevalence of online buying scam and fraud scores between the groups. Moreover, Wilcoxon W's tool creates a pooled ranking of all observed discrepancies between the two dependent metrics. The usual normal distributed z-value is employed to test for significance.

The materials used for this study are the Survey questionnaire by Ipsos (2020) in the Final Report of the European Commission: Survey on "Scams and Fraud Experienced by Consumers" using QuestionPro Social Media Questions Free Template (2022) and Whitty (2019), Predicting Susceptibility to Cyber Fraud Victimhood, and 33 Social Media Survey Questionnaire by Formplus (2022), was adopted and modified. The questionnaire is divided into two parts; first part deals withthe profile of the respondents; and second part is the prevalence of online buying scam and fraud exposure, with two indicators: lifestyle and routine activity.

RESULTS AND DISCUSSION

As to the profile of the respondents, results revealed that the majority of the respondents who experienced online scams and fraud were in the age range of 20 to 21 years of

age, and the least were aged 26 years and above. Females are mostly scammed, and those in the third year level, while the least scammed are those in the fourth year level.

As to the prevalence of online buying scams and fraud exposure, respondents would likely become victims based on their lifestyle and daily routine activities. This is supported by the idea of Vakhitova et.al., (2019), which state, the risk to cyber abuse victimization is affected predominantly by the lifestyle and routine activities of the victims. Their lifestyle of being exposed online, together with any other online interactions with strangers, can increase the likelihood of risk to scams, fraud and a mixed type of cyber abuse.

Likewise, as to prevalence of online buying scams and fraud exposure in terms of lifestyle, the result reveals that social media has an influence on respondent's behavior, oftenness of their scrolling time in online shopping sites or buying apparel, gadgets, or other goods and services online; persuaded due to opinion about the values and usage but it turned out untrue; being motivated to buy products to maintain or pursue a certain lifestyle; and the presence of brand social media to influence their purchasing decision; is described as most frequently, and are the main lifestyle contributor that leads to them being a victim to online buying scam and fraud exposure. Such indicator is also followed by lifestyles that refers to ordering a product online due to the participation of famous people, but it turned not, and usually looking through social media influencers or checking at what is trending first when choosing goods/services to buy; concerning being attracted to a product that has alleged better position among competitor but it turned not; as well as buying what they thought was a good deal, but it is never received, or the

goods/services turned out to be fake or non-existent, are frequent lifestyle indicators that lead to their exposure to online buying scam and fraud, respectively. Utami et al. (2022) indicate the millennial generation, which makes up the majority of the global population, prefers a modern buying lifestyle. It is much different from previous customers, who tend to favor and are used to a traditional shopping lifestyle. People follow along with trends, and so does their lifestyle; hence they consume what is trending on the market or by online shopping.

As to prevalence of online buying scam and fraud exposure in terms of routine activity, results depict indicators described as very frequently, such as: usually writing down their accurate personal information in online shopping websites; tending to spend a lot of time in an online shopping website when looking for a specific product/service that would be much cheaper than the other shop; usually using their mobile phone and its mobile data when communicating; or doing transactions such as banking and shopping; in terms of them, being contacted by phone, face to face, by email or by another means, by someone pretending to be from a legitimate organization such as a bank, telephone or internet service provider, or government department, and asked to provide (or confirm) personal information; and buying products/service online at least a few times in a month; in addition to feeling time constrained, so instead of buying in physical stores, they tend to turn to buy online due to its door-to-door delivery service; furthermore, often streaming media (movies, music, etc) and product pop up ad can sometimes entice them, respectively. While in terms of being contacted by someone pretending to be from a legitimate organization, such as a bank, internet provider, or government, who

claimed there were problems with their account or other documentation and threatened them with harm if they did not pay to resolve the problem, obtained an interpretation of frequently. Likewise, in terms of being approached by phone, face to face, by email, by another means or they accessed a website and were informed that they had a computer or internet problem, they were asked for personal details and bank or credit card details to have the problem solved; as wells as ordering free or relatively cheap products or services, but was tricked into a costly monthly subscription, garnered an interpretation of occasionally. Data proved the idea of Nickerson (2022), stating that people who have involved on the Internet in their routine activities are perfect prey to fraudsters due to the absence of proper protection and security against them due to the lack of a capable guardian.

As to the significant difference in the level of prevalence of online buying scams and fraud exposure among business administration students when analyzed according to age, in terms of lifestyle, with a p-value of 0.634, and routine activity, with a p-value of 0.332, it denotes that there is no significant difference on the lifestyle and routine activity and the exposure to online buying scam and fraud among the respondents despite its non-uniformity in an age where the p-value is greater than the alpha value of 0.05 hence, does not reject the hypothesis. This validated the information that most online fraud attempts in the Philippines were commonly targeted toward younger people (Crismundo, 2021). However, it should also be noted that an individual's characteristic, lifestyle, and routine activity affects their behavior in buying online. Hence, regardless of age, impulsive people and those with a lack of understanding of online scams and fraud are at risk of being involved in cybercrime

victimization (De Kimpe et. al., 2018).

As to the significant difference in the level of prevalence of online buying scams and fraud exposure among the respondents when analyzed according to sex, in terms of lifestyle, with a p-value of 0.247, and routine activity, with a p-value of 0.305, it points out that there is no significant difference in the lifestyle and routine activity on the online buying scam and fraud exposure among the respondents despite its differences in sex since the p-value is greater than the alpha value of 0.05; thus we do not reject the hypothesis. This guarantees Whitty's (2019) claim that activities online function as a mediator between demographic factors like age and sex and the chance of being targeted for online scam and fraud.

Additionally, as to significant difference in level of prevalence of online buying scam and fraud exposure among respondents when analyzed according to year level, in terms of lifestyle, with a p-value of 0.215, and routine activity, with a p-value of 0.416, it implied that there is no significant difference in the lifestyle and routine activity on the online buying scam and fraud exposure among the respondents despite the distinction in year level since the p-value is greater than the alpha value of 0.05 hence does not reject the hypothesis. This substantiates the idea that people with higher levels of education were more likely to engage in habitual behaviors and routine activities that could possibly introduce them to online scams and fraud. This demonstrated that the level of education is not a defense against being a victim of scams and fraud (Whitty, 2019).

Furthermore, as to the significant difference in the level

of prevalence of online buying scams and fraud exposure among respondents when analyzed according to their program, in terms of lifestyle, with a p-value of 0.149, and routine activity, with a p-value of 0.079, it exhibits that there is no significant difference in the lifestyle and routine activity and the online buying scam and fraud exposure among the respondents despite heterogeneity in the program since the p-value is greater than the alpha value of 0.05; thus we do not reject the hypothesis. The result was backed by Whitty (2019), stating when considering repeat victimization, the psychological or socio-demographic aspect is not an essential distinguishing factor between one-time or recurring victims. Therefore, people can be exposed to scams and fraud regardless of psychological and socio-demographics as long as people are involved with the Internet.

CONCLUSION AND RECOMMENDATIONS

It is concluded that no matter what age bracket the students are, they are equally exposed to online buying scam and fraud. Additionally, there is no significant difference between online buying scam and fraud exposure levels in terms of sex because both male and female can become a victim of online buying scam and fraud when they make purchases online, the same with students' year level, and program because whenever they patronize products and/or services or entertained information and advertisements online that tend to persuade them to buy online, they would likely be exposed to online buying scam and fraud. Likewise, it is concluded that the prevalence of online buying scam and fraud, do not differ as to one's lifestyle and routine activities since data shows no significant difference. This may be the case because online scammers are becoming technologically

advanced that they are not easy to be detected. The scenario is added with lack of government facilities to track down and control online merchant's schemes, making anyone who relies on online shopping a potential target of scams and fraud. As such, it is generally concluded that anyone who patronizes buying products online might be exposed to online scam and fraud.

Based on the findings of the study, the following recommendations were given: To Students, it is recommended to be extra careful and fastidious and thoroughly examine the product advertised on online platforms, such as checking the customer review. Also, they should not immediately respond to the messages sent to their account when sources are unknown. Likewise, it is recommended that they should only purchase or order online products from a reliable source/s or supplier to avoid being a victim of online scams and fraud. Further, they should put it in their minds that not all products and messages advertised or posted online are legitimate, authentic and accurate, as promised. They should manage their social media settings and keeppersonal and other private information not posted on social media sites as much as possible. They should use a strong password when using public WiFi Networks and install a Virtual Private Network (VPN) app on their gadgets to mask the device's Internet Protocol (I.P.) address.

To Professionals, the researcher recommends that when dealing with online transactions, they should keep in mind the use of strong passwords, have the software constantly updated, and strengthen home network, such as using strong encryption passwords. When using a public WiFi Network, it is advisable to use and install a Virtual Private Network (VPN)

app in gadgets to mask the device's Internet Protocol (I.P.) address, encrypt data and route the information and internet activity through a secure network. Likewise, in order to bolster protection against online scams and fraud, and even identity theft, it is suggested that professionals should manage social media settings and keep personal and other private information posted in social media sites locked since some known possible security questions posted in online user's account can enable cyber criminals to hack the victim's accounts. Also it is recommended to the Government Legislature that they should pass a law that would strongly regulate and penalized online scammers and those who employ fraud. The penalty should be heavy, and the implementation should be robust to help protect the general public against those scheming and fraudulent activities in online setting, especially those who target students who only rely upon their parents for support.

In addition, to the Academe and its personnel, this university and other educational institutions both private and government, local government units and other agencies, it is recommended that they should make an intensive information campaign among their students, specifically on improving their financial attitude and propensity to buy online and respond to unsolicited messages on the internet to avoid being a victim of online buying scam and fraud. A seminar campaign should always be on Anti-cyber Crime Act, Data Privacy Law, and other informative topics related to typical computer and internet cybercrime and fraud. They have to facilitate educating people through seminars and other information campaigns about cybercrime and crime prevention strategies.

Further, to Business Owners, it is also recommended that they should also consider their employees' welfare and have an awareness campaign teaching them about cybercrime and crime prevention strategies. In addition, it is suggested that companies must have their computers and gadgets adequately protected by having the system constantly updated, and if possible, utilize making a detailed System Security Plan (SSP) to keep the company's data secure and to respond and counter any malicious attacks in case of a security breach. Furthermore, companies should implement cyber security training among employees since they are the ones who receive some first-hand information and documents from their own computers. Lastly, for Future Researchers, it is recommended that they utilize this study as the basis for future studies related to this topic and should investigate and delve into some aspects not covered by this study.

REFERENCES

Crismundo, K. (2021). Digital fraud attempts in PH rise amid pandemic. Philippine News Agency. Retrieved from https://www.pna.gov.ph/articles/1134735.

Daroch, B., Nagrath, G., & Gupta, A. (2021). "A study on factors limiting online shopping behaviour of consumers", De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail!: Explaining individual differences in becoming a phishing target. TELEMATICS AND INFORMATICS, 35(5), 1277–1287. Retrieved from https://doi.org/10.1016/j.tele.2018.02.009.

Ipsos. (2020). Survey on "Scams and Fraud Experienced by Consumers".Final Report.

Nickerson, C. (2022). Routine Activities Theory. Retrieved from https://www.simplypsychology.org/routine-activities-theory.html.

Utami, S., Anzar Huthasuhut, M. F., & Lubis, P. H. (2022). The Influence of Brand Image and Lifestyle on Purchase Intention Mediated by Consumer Attitude on Personal Care Products with Regional Comparison as Multigroup Moderator (Study on Consumers in Banda Aceh VS Lhokseumawe). International Journal of Scientific and Management Research, 05(08), 43–57. Retrieved from https://doi.org/10.37502/ijsmr.2022.5804.

Vakhitova, Z., Alston-Knox, C., Reynald, D., Townsley, M., & Webster, J. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? Computers in Human Behavior. vol. 101, pp 225-237.

Whitty, M. (2019). "Predicting susceptibility to cyber-fraud victimhood", Journal of Financial Crime, Vol. 26 No. 1, pp. 277-292. Retrieved from