Original Research

MODUS OPERANDI: CYBERCRIME IN THE MIDST OF PANDEMIC

Jeric Galvan[1], Jade F. Garalza[1], Joemari V. Grabillo[1], Patrick Art A. Robles[1], Troy G. Jerald[1] and Melchor L. San Miguel[1] and Dr. Desire G. Estrada[1]

[1] School of Criminology, Emilio Aguinaldo College, Manila

ABSTRACT

Cybercrime is defined as criminal activity involving a computer, an internet connection, or a local area network. However, the COVID-19 has resulted in a significant computerized change, with innovation being at the edge of countries' reaction to the crisis. The main objective of the study is to discuss the concept of cybercrime in the midst of the pandemic, what are the techniques and strategies of the Philippine National Police Cybercrime Division in resolving the cybercrime and how they face these kinds of issues. A phenomenological study under a qualitative approach was used to conduct the study. A total of 20 victims, specifically in Pasig City from different types of cybercrime are the main criteria of the respondents. A validated interview guide was utilized to gather the desired data of the researchers. Respondents with a total of 16 online scams, 2 anti-photo and video voyeurism, 2 identity theft are the individuals who did not report their case to the ACG (Anti-Cybercrime Group). From the record of EDACT (Eastern District Cybercrime Team), the cases of cybercrime consist of 1 illegal access, 2 identity theft, 1 access device act, 4 anti-photo and video voyeurism, 1 threat, 2 Estafa. The results revealed that online Estafa is the frequent type of cybercrime that occurred during the Covid-19 pandemic. Moreover, a large number of victims still chose not to report their cybercrime case because they identified it to be a waste of time and moreover the victims reported that they still have high hopes to regain what had been lost highlighting the relevancy of cybercrime issues during the course of the pandemic.

Keywords: Modus Operandi, Cybercrime, Covid-19 pandemic, Social media

INTRODUCTION

Social media is defined as an internet-dependent application which was established to promote social intercommunication, and using and developing information through society (Kapor et al., 2017). According to Maras (2016), numerous nations have created laws that are particularly outlined to bargain with cybercrime. Some of the common reasons are for communication, marketing and entertainment. Unfortunately, aside from the positive side, some people take advantage of social media's power and utilize it in an against the law action. As stated by Brush et al (2021), cybercrime is defined as any criminal activity which involves a computer, networked device or a network. This type of crime was increasing in the world by organizing cyber-attacks. Devices can be used in illegal activities that can commit fraud, pornography, stealing identity and bullying. The offender was called cyber criminals or in other terms hackers that make a lot of money by using their computers and other devices. Currently, this practice has been very familiar since people have a huge amount of time to browse devices and some of them become vulnerable in some ways.

Cybercriminals frequently utilize malware and other specialized software to carry out their illicit activities. However, social engineering is often an essential and important component for executing most types of cybercrime (Rouse et al., 2020). Initially, cybercrime activity often remains undetectable; however, its effects eventually surface, making the crime public. This process typically involves the illegal transfer of data or information that is of confidential value to individuals or groups. Computer crimes began in the 1960s when computers were first introduced into corporations and government agencies however in recent times it is now more prevalent due to the internet.

The continuous evolution of technology, particularly the expansion of the Internet of Things (IoT), has significantly widened the scope of cybercrime, which is now considered the most common type of crime. This phenomenon is driven by the increasing digitization across all sectors and the heavy reliance on Information and Communication Technologies (ICTs) for essential services like transportation and electricity. IoT devices, such as medical sensors and smart cars, pose a unique security challenge due to their limited size and lack of innate security, making them difficult to protect with traditional methods (Cloud Security Al, n.d.).

In the current digital age, cybercrime has risen to become the most common type of crime, exclusively carried out through the internet (Cloud Security Al, n.d.). The spectrum of hostile activities is vast, ranging from overt acts like computer intrusion, the distribution of viruses, and website defacement, to more subtle attacks like denial of service (DoS) (Yar & Steinmetz, 2020). While the primary motivator for the majority of cybercriminals is profit, many attacks are executed directly against devices, aiming to destroy or disable them (Cloud Security Al, n.d.).

Focusing on the elements between governments and enormous tech, on cybercrime, and on disinformation and fake news, this paper looks at a few of the dangers that have been highlighted and exasperated as social orders have transitioned at speed to a more virtual way of living. The COVID-19 widespread has been called the ‘great accelerator’ of computerized change, with innovation at the bleeding edge of countries’ reaction to the crisis. The encounter of the past year has underscored that tech administration must be based on human-centric values that ensure the rights of people but to work towards an open public.

According to data collected by partners of the referenced police institution, the early stages of the pandemic, specifically between January and April of 2020, saw a massive surge in COVID-19 related cybercrime. This period alone recorded 907,000 spam emails, 737 malware incidents, and 48,000 malicious URLs exploiting the crisis. Cybercriminals rapidly adapted their modus operandi during this emergency, shifting focus from individual users to large companies, governments, and critical infrastructure. These larger targets, burdened and potentially collapsing under the stress of the pandemic, became more vulnerable and lucrative. However, this adjustment did not spare private clients from attacks. The sudden necessity for companies and employees to rapidly implement new systems, applications, and processes for remote work also created a fertile new target for mass assaults. As noted in earlier reports, cybercriminals are constantly active, monitoring situations like this emergency—one of the most profitable for the criminal world—to facilitate their criminal activity. Experts anticipate that attackers will continue to exploit vulnerabilities arising from the widespread adoption of teleworking, in addition to launching phishing campaigns that target the public by impersonating legitimate health or administrative organizations to steal sensitive banking and personal data. Furthermore, crucial work, such as the research and production of vaccines, remains highly vulnerable to ransomware attacks or information theft that could disrupt development, logistics, or manufacturing processes. This Interpol-related study provided a clear snapshot of the cybercrimes prevalent during the pandemic.

At least 121 charges have been recorded against 87 individuals for illicit acts extending from spreading disinformation on the Web to unlawful online deals of restorative supplies, according to the Philippine National Police. As stated by the PNP Chief Gen. Guillermo Eleazar (2020), separated from upholding well-being and security conventions, police proceed to go after fiendish individuals who are making a benefit and taking advantage of our fellowmen in this time of the COVID-19 pandemic. To support the statement, based on the information from 9, 2020 to Eminent 9, the Criminal Examination and Location Gather and the Anti-Cybercrime Gather (ACG) have recorded 87 criminal complaints against 52 people for spreading fake news; three online trick complaints against two people; and 31 criminal complaints against 26 people for online profiteering, overpricing, accumulating and unauthorized offering of therapeutic supplies within the diverse prosecutor’s workplaces nationwide. The PNP has escalated its observation of cyber wrongdoings as most individuals are working.

Online scams and Phishing - Risk on-screen characters have reexamined their normal online tricks and phishing plans. Due to COVID-19, there are many people imitating the government and specialists. Cybercriminals take advantage of the people to get personal information. Around two-thirds of part nations that reacted to the worldwide cybercrime study detailed a noteworthy utilization of COVID-19 topics for phishing and online extortion since the flare-up. Disruptive Malware (Ransomware and DDoS) - Cybercriminals are progressively utilizing troublesome malware against the basic foundation and healthcare teach, due to the potential for tall effect and monetary benefit. In the primary two weeks of April 2020, there was a spike in ransomware assaults by numerous risk bunches which had been generally torpid for the past few months. Law requirement examinations appear the lion's share of aggressors evaluated very precisely the most extreme sum of emancipation they might request from focused on organizations.

Information Collecting Malware- The arrangement of information collecting malware such as Farther Get to Trojan, data stealers, spyware, and managing an account Trojans by cybercriminals is on the rise. Utilizing COVID-19 related data as a draw, dangerous on-screen characters invade frameworks to compromise systems, take information, redirect cash and construct botnets.

Noxious Spaces- Taking advantage of the expanded request for restorative supplies and data on COVID-19, there has been a noteworthy increment of cybercriminals enlisting space names containing catchphrases, such as “coronavirus” or “COVID”. These false websites support a wide assortment of malevolent exercises counting C2 servers, malware arrangement, and phishing. February 2020, a 569 percent development in malevolent enrollments, counting malware and phishing, and a 788 percent development in high-risk enlistments were identified and detailed to INTERPOL by a private division accomplice. Deception- An expanding sum of deception and fake news is spreading quickly among the open. Unconfirmed data insufficiently caught on dangers, and trick speculations have contributed to uneasiness in communities and in a few cases encouraged the execution of cyberattacks. Nearly 30 percent of nations that reacted to the worldwide cybercrime study affirmed the circulation of wrong data related to COVID-19. Inside a one-month period, one nation detailed 290 postings with the larger part containing concealed malware. There are two reports of deception being connected to the unlawful exchange of false restorative commodities. Other cases of deception included tricks through portable text messages containing 'too great to be true' offers such as free nourishment, extraordinary benefits, or expansive rebates in grocery stores.

Internet scams are constantly evolving and can take on a wide variety of forms. Generally, the phrase refers to someone who uses online services or programs to scam or exploit victims, usually for financial benefit. Cybercriminals may communicate with potential victims via personal or professional personal emails, social media sites, online dating sites, or other means in an attempt to collect financial or other vital personal information.

The top two countries with the most prominent online fraud are Mexico and the United States of America. According to Touryalai, H. (2021), Mexico and the United States are much more susceptible to it, with 44 percent and 42 percent of respondents, respectively, reporting having been a victim of card fraud. While debit and credit card fraud are more prevalent than ever, it is considerably more prevalent in particular nations, such as the United States. The United States ranks highly on the list of fraudsters: It is not a requirement of the EMV standard. Euro pay, Mastercard, and Visa are abbreviations for EMV. It is a European standard that most nations adhere to maintain card security via microprocessors in card transactions.

During May 4, 2000 a student from the AMA Computer College in the Philippines created a computer virus called “ILOVEYOU” virus or also known as “Love Bug”. The ILOVEYOU virus was spread through emails and it is designed to spread the virus. That computer virus has damaged ten million personal computers in just one day and almost 5.5 to 8.7 million Dollars was the damage of the virus.

As reported by the Philippine Congress enacted Republic Act No. 10175 or "Cybercrime Prevention Act of 2012" any crimes committed against and by means of computer systems will be subjected to penal substantive rules, procedural rules and also rules on international cooperation.

In the year 2019, the number of cybercrime incidents in the National Capital Region (NCR) in the Philippines will reach the highest level, which is that SMS or Text scams have approximately 2.7 million victims. Other incidents committed in the Philippines were hacking, phishing and cyberbullying. (Statista Research Department, 2021). Philippine National Police (PNP) cybercrime has increased since 2010 and yearly it was rising in our country. Criminal Investigation and Detection Group (CIDG) show that the PNP reported 4,673 cybercrimes and 527 cybercriminal cases were reported in the year 2006, during 2005 to 2010 2,624 cases were reported. The PNP has investigated 195 computer crimes, the cases are commonly like credit and debit card fraud, Internet pornography, violation of copyright laws and other crimes committed by using computers.

They also released a report stating that Filipino victims were increased to the online criminal activities. Filipinos have fallen to attacks by the cybercriminals that included malware invasion, online scam, sex trafficking, and online networking usually in Facebook and almost 16 million users in the country.

As indicated in the Philippines' National Security Policy (NSP) 2017-2022, Cybercrime is today's fastest rising economic crime due to the increasing number of criminals that the internet provides using speed, convenience, and anonymity. Thus, the government's 12-point national security agenda identifies the importance of informational and cyber security goals of the country which aims to guard classified and sensitive government records including the state secrets of espionage, and to protect the country from the cyber-attacks which can affect the private and public infrastructure (Castillo, 2020) The transformation of technology has a big impact on the global economy and to be a guide to information and communication (Li, 2021).

Technology makes it easier for a lot of people that are described as "a borderless world" which may lead to new ways and also in modern times. The adoption of e-services in a country where such implementation is critical to the delivery of fundamental services to the public presents a security problem. E-services will fail unless there is a guarantee of privacy and security for information circulating on the internet. The threat of cybercrime prevents the reach of e-government and risks the attainment of the country's national aims of improving the socio-economic environment for the residents. In essence, it's the equivalent of posing a serious threat to national security. The study aims to examine the effectiveness of law enforcement on the protection of children victims of cybercrime in Indonesia. The method used is empirical legal research, which examines the law on social phenomena. The collecting data were from primary and secondary data. The primary data was based on the related institutions in handling child victims of cybercrime, and secondary data were collected through questionnaires administered to 4 (Four) selected Provinces samples (Djanggih et al., 2018). The results showed that the form of cybercrime experienced by the child as a victim dramatically increases every year and still seems to be weak in law enforcement. Public response to law enforcement from the aspects of law Substance, law enforcement, infrastructure facilities, inter-agency coordination is ineffective, and public responses to the handling of victims of cybercrime must be quickly addressed. This is a form of state responsibility for the protection of children victims of cybercrime. Thus, children can live and grow up to avoid the crimes that occur through cyber development.

The children could be a victim of cyberbullying or they could be cyber-bully if they are guided by their parents. Konradt et. al. (2016) believed that cybercrime is one of the most important security topics, and will continue to emerge as a more critical security threat within the next few years. Among the different attacks, phishing is of special interest because of its negative impact on the economy. A simulation study is to be developed based on the work of Fultz and Gross lags. To extend their analysis of cybercrime from an economic view, the researchers customized their model and used it as the basis for our analysis. Based on the data from recent literature, the assessment gives insights into the perpetrator's behavior and allows us to quantify the effectiveness of countermeasures. Due to the fact that mainly risk-seeking persons are responsible for these attacks, countermeasures aiming at increasing the penalties are not very effective. The researchers discovered that better control of dark markets to prevent the trading of stolen data has a much higher impact. In general, the results of the simulation can be used to analyze the perpetrator's economic motives and to establish a basis for effective countermeasures. The online scam nowadays is very alarming. Many people are using online transactions because of the pandemic to avoid contact with another person. But when people are using online transactions it is more different in person. While using this way of communication or mode of payment there is a risk behind that. There are a lot of scams in online transactions, the first is the phishing scam. Phishing is a type of cybercrime that involves the use of false emails, websites, and text messages to steal personal and business information.

The main objective of the study is to discuss the concept of cybercrime in the midst of the pandemic, what are the techniques and strategies of the Philippine National Police Cybercrime Division in resolving the cybercrime and how they face these kinds of issues. This study aims also to have a further understanding of why people are inclined to this kind of activity. The researchers want to determine the impact of cybercrime in society nowadays because as many people transact online due to the COVID-19 pandemic and some of them are cyber criminals that want to take advantage of the people who are using online transactions. The researchers want to gain and share knowledge about the different types of cybercrimes some of these are online scams, phishing, noxious spaces, deception, information collecting malware, etc. This study is therefore conducted in order to determine the different modus operandi of offenders in the perpetration of cybercrime. While also giving knowledge, awareness and possible recommendations to lessen the occurrence of cybercrimes.

A developed theory from Jaishanker, 2017 called Space Transition Theory was made in order to explain how crimes on the internet are made. It proposes a comprehensive framework for understanding how individuals shift between physical space and cyberspace in the context of criminal behavior, suggesting that the dynamics of the online environment fundamentally alter criminal propensity and opportunity. Firstly, the theory posits that individuals who have repressed criminal behavior in the physical world are more likely to commit crimes in cyberspace, which they would otherwise avoid due to their status and position offline. This is enabled by the online environment's characteristics: Identity Flexibility, Dissociative Anonymity, and a lack of deterrence factor collectively offer offenders the choice and comfort to engage in cybercrime. Furthermore, the relationship between the two spaces is reciprocal: criminal behavior initially displayed in cyberspace is likely to be imported into physical space, and, conversely, criminal activities in physical space may be exported to the digital realm. The theory also notes that the intermittent ventures of offenders into cyberspace, combined with the domain's dynamic spatio-temporal nature, provide criminals with opportunities to evade detection and escape consequences. Regarding collaboration, the theory states that strangers are likely to unite in cyberspace to commit crimes in physical space, while associates from the physical space are likely to unite to commit crime in cyberspace. Finally, the theory suggests that individuals originating from a closed society are more prone to commit crimes in cyberspace compared to those from an open society.

METHODOLOGY

A phenomenological study under a qualitative approach will be utilized for the present study. In this kind of research design, it looks at the experiences of the participants under the said phenomenon. It describes through interview and observation to the participants (Naresh, 2020). In context to this research study, the phenomenological design is best fit in order to attain the objective of this study to know their experience in cybercrime. This is to further investigate the modus operandi specifically during the midst of pandemics.

Participants for this study were specifically recruited based on their characteristic of frequently buying and transacting online through a purposive sampling technique. This selection criterion is critical given the current environment where the pandemic and resulting lockdowns have pushed people toward heightened online activity. Research by Ngo et al. (2020) demonstrated a significant link between online activity and cybercrime victimization. Specifically, their findings showed that five of the seven types of cybercrime investigated—including computer virus infections, harassment by known individuals, unwanted pornography, sex solicitation, and phishing—were significantly related to various online frequency, activity, and posting variables. These variables included the number of internet hours spent online, six specific online activities (banking, reading news, shopping, planning travel, socializing, and communicating with strangers), and three types of personal information posted (phone number, home address, and other information). Reflecting this trend, the present study recruited a sample of at least ten (10) online consumers who have been victims of cybercrime.

The study was conducted at Barangay Pinagbuhatan, Pasig City, 1602 Metro Manila. The effects of the outbreak of pandemic and its continuing threats to people’s lives prevented the researchers from having the exact data as to the number of families needed. From the large target population, a total of twenty (20) participants were included.

An Interview guide was used for the respondents to have further knowledge about what are things that a cybercriminal does to accomplish a cybercrime or online scams. And, to know their experiences about the said cybercrime.

Furthermore, an online interview was conducted via google meet and a one-on-one interview, in order to ensure confidentiality to his/her probable answers about their experiences. Interviews lasted between 15-20 minutes depending on the experience of the participants. The interview was conducted online to follow the safety protocols of the government and to have a non-contact interview for the safety of both parties.

Participants have the right to withdraw from the study at any stage if they wish to do so. The researchers will also ensure that the participation is voluntary. No harm will be done to the participants. The information provided by the participants shall be used only for the purpose of the research and shall not be disclosed to other people. Regarding the study, the participants were informed with the purpose of the study. The participants who are involved in the study can access to the collected data by the researchers, being fair the researcher's participant will also own their personal copy of the consent and they also have the access to the latest finding of the study as they requested.

All observations, interviews, and focus groups were verbatim transcribed. After that, the transcripts were unitized, which split the material into independent pieces of information that could stand on their own. The experiences that will be mentioned by the respondents/participants will have an impact on this study because they are ones who experience the said case of cybercrime. In general, qualitative data analysis is thought to be a nonlinear, iterative process.

RESULTS AND DISCUSSION

Based on the results of the survey, the most frequent cybercrime that the victim experienced as shown in Figure 1 while Figure 2 shows the most frequent cybercrimes that have been reported to the Eastern District Anti-Cybercrime Team.

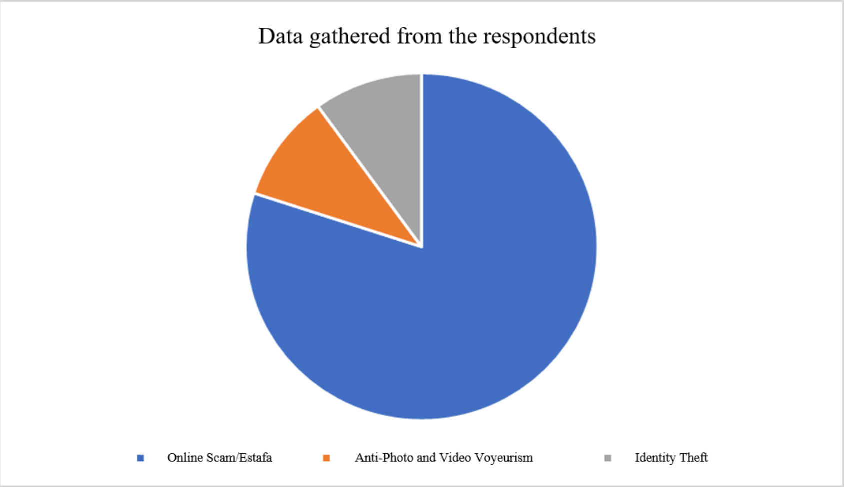

Figure 1. Summary of the data obtained from the respondents

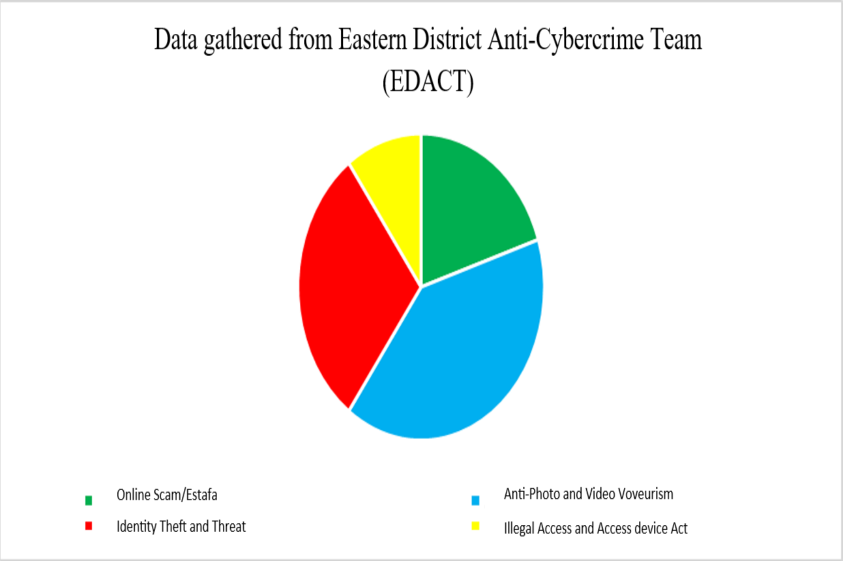

Figure 2. Frequent type of Cybercrime (for EDACT)

DISCUSSION

Cybercrime is widespread nowadays in the midst of pandemic because as we all know many of us depend on our gadgets, using social media, paying bills and buying everything we want using just our mobile phones. These are the orders that will result in the consumer's loss of money and time.

An online scammer pretends to be a legitimate seller using a fake ad on an authentic e-commerce platform, social media site, or a fake website. The fraudster tricks a customer into paying for a non-existent product and then delivers nothing and runs away with the money. Crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information.

Identity theft- When someone steals your personal information in order to commit fraud, this is known as identity theft. Your information could be used to apply for credit, file taxes, or obtain medical care. These actions can negatively impact your credit score, costing you time and money to repair.

Computer-related identity theft - is defined by RA 10175 as the unauthorized acquisition, use, misuse, transfer, possession, change, or deletion of identifying information belonging to another person, whether natural or legal.

Criminals may "shoulder surf" in public locations, watching you type in your telephone calling card number or credit card number from a nearby position, or listen in on your discussion if you give your credit card number over the phone.

Criminals may retrieve applications for "pre-approved" credit cards that you discard without tearing up the contained paperwork and try to activate the cards for their usage without your knowledge if you discard them without tearing up the attached materials. Furthermore, if your mail is sent to a location where others have easy access to it, criminals may easily intercept it and redirect it to another site.

Many people respond to "spam" – unsolicited E-mail – that promises them something in exchange for identifying information, not realizing that the requester, in many circumstances, has no intention of delivering on his offer. Criminals have allegedly exploited computer technology to steal enormous amounts of personal data in some circumstances.

Financial identity theft- When someone utilizes another person's information for financial benefit, this is the most common type of identity theft. A fraudster could, for example, steal money or make transactions using your bank account or credit card details, or use your Social Security number to obtain a new credit card.

Synthetic identity theft- Fraudsters can establish bogus identities using either fabricated or real information, or a combination of the two, in synthetic identity theft. An identity thief might, for example, use a valid Social Security number but a name that isn't related to it. Children and the deceased are particularly vulnerable because their Social Security numbers are rarely used.

Medical identity theft - is a serious problem. A fraudster will use your personal information to obtain medical treatment in your name in medical identity theft.

Fake booking is a type of a prank to several riders, riders will receive an order, which usually costs more than 1,000 pesos. Some of the items were food, clothes and other things that can be delivered using a motorcycle. When the rider arrives in the place where he/she will receive the item. After he/she received the item from the sender. When the rider also arrives at the place of the receiver, the receiver asks the rider to wait for a minute but it comes to an hour then also the sender will block the number or the contact from the rider. Because of that the rider loses earning, time and inconvenience on the side of the rider.

Fake booking is a type of cybercrime that makes a huge impact to those riders like Lalamove, Grab and others delivery services in the Philippines. Food and grocery delivery service providers in the Philippines are part of essential industries during the peak of Pandemic. They are mostly motorcycle riders the government allows to work under ECQ quarantine restrictions. Because the demand of the delivery services has risen, the fake booking cases also increase in the Philippines. Because of the amount of fake booking cases Hon. Alfredo Gardin Jr. introduced **House Bill No. 6958**, or the **Act Providing Protection to Individuals Engaged in the Food and Grocery Delivery Services**, to Philippine Congress. This bill will protect the delivery rider from the scammers because usually it is a type of transaction that is cash on delivery or also known as COD.

ANTI PHOTO and VOYEURISM ACT- Spreading the nude photos or sex videos of another without his or her consent is punishable under Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009. The use of technology in this modern society has brought forth a borderless world. Thus, sharing of information knows no bounds and has enabled us to communicate to a wider range of audience. As the adage goes, the world is your oyster. However, these technological advances have also been used by unscrupulous individuals to victimize others. Private photos and videos which are shared intimately to trusted persons are being used to exploit these private moments. Good thing the Philippines finally enacted in 2009 RA 9995 which punishes photo or video voyeurism.

With all those modus operandi that have been enumerated and gathered from the respondents there are techniques and strategies that our PNP Cybercrime Divisions implemented for that case. First in discussion is to conduct seminars and webinars to different barangay and cities to give awareness about the cybercrimes that happens in the midst of pandemic, with this people will be aware and will also result to lessen and minimize the victimization of cybercrime, Second, The ACG or the Anti-Cybercrime Group have a Facebook page and Website in order to post infographics to give guideline to the people that are very active in the cyberspace, reading and understanding these guidelines we help the people to prevent being a victim of cybercrime. Third, As the victim reported his/her case in the anti-cybercrime division, the PNP officer immediately gather data from the respondents by doing a police blotter to locate who is the recipient of the money, also if they seize evidence from the suspect, they immediately file or apply a cybercrime warrant to gather all the data inside the mobile phones or personal computers. The EDACT also has a Forensic Expert that is responsible for the collection of the data and to present in court, the forensic expert is also the expert witness when it comes to trial or hearing of the case. Lastly, the EDACT operates an entrapment operation for the future apprehension of the cybercriminals, this is one way to lessen the cybercriminals in our country because cybercriminals are very hard to apprehend for the reason that they are hiding from their technologies.

CONCLUSION

The study disclosed that there are different types of cybercrime that are happening during this covid-19 pandemic. Most of the respondents chose not to report to EDACT since according to them, it is just a waste of time, lack of eagerness, and having high hopes that they will recover what they have lost. Cybercrime nowadays possess a higher number of cases than before since many people are more engaged in virtual worlds. Cybercrime issues have been relevant during the time of *Covid-19* pandemic. People are inclined on online transactions more than ever. Doing transactions online has proven to be more convenient and safer than going out due to the pandemic. Therefore, some of the measures should be taken by a person to avoid such crimes. The vigilant behavior and following the guidelines are only helping aids which can reduce the occurrence of cybercrime. We should always focus on awareness as “Prevention is better than cure”.

RECOMMENDATION

Participants are encouraged to be more vigilant, always check the legitimacy of the seller, read the comments or review of the recent transactions and never disclose your personal details to prevent your personal information from being captured. The people in the virtual world should take more time to read and analyze the different guidelines and prevention in being a victim of cybercrime to at least lessen the cybercrime victimization.

In line with that, The Anti-Cybercrime Group has a Facebook page and websites that are giving guidelines and prevention tips for the people inclined in the virtual world. It is recommended to develop new strategies that may align to the future apprehension of the cybercriminal because it is very relevant now that we are facing this kind of pandemic and people are more active in social medias, there must be more effective and efficient techniques to be utilized to lessen the occurrence of cybercrime in our country.

ACKNOWLEDGEMENTS

Sincere gratitude is given to Dr. Desire G. Estrada for her continuous support and encouragement and the Chief of Eastern District Anti-Cybercrime Team (EDACT) PMAJ Ely D. Compuesto II and Pat Fave Cadano for their time and knowledge.

REFERENCES

A.C.G.P.N.P.G.O.V.P.H. (2013, August 8). CYBERCRIME THREAT LANDSCAPE IN THE PHILIPPINES. Https://Acg.Pnp.Gov.Ph/Main/about-Us/20-Publications/42-Cybercrime-Threat-Landscape-in-the-Philippines.Html. Retrieved from https://acg.pnp.gov.ph/main/about-us/20-publications/42-cybercrime-threat-landscape-in-the-philippines.html

Alghamdi, M. I. (2020, June 23). *A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide*. International Journal of Engineering Research & Technology. Retrieved from https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-.
Analyze qualitative data " Pell Institute. Evaluation Toolkit. (n.d.). Retrieved from http://toolkit.pellinstitute.org/evaluation-guide/analyze/analyze-qualitative-data/.

Brush, K., Rosencrance, L., & Cobb, M. (2019, December 23). *What is cybercrime? definition from searchsecurity*. SearchSecurity. Retrieved from https://searchsecurity.techtarget.com/definition/cybercrime.

Caliwan, C. L. (2020, September 22). Public warned vs. con artist using name of PNP chief. Https://Www.Pna.Gov.Ph/Articles/1116188. Retrieved from https://www.pna.gov.ph/articles/1116188

Castillo, C. L. M. (2020, January 30). Defending the Philippines' Cyberspace Amid COVID-19. Http://Www.Ndcp.Edu.Ph/Index.Php/Defending-the-Philippines-Cyberspace-amid-Covid-19/. Retrieved from http://www.ndcp.edu.ph/index.php/defending-the-philippines-cyberspace-amid-covid-19/

Cloud Security Alliance. (2021). *Internet of things working group: CSA*. Working Group | CSA. Retrieved from https://cloudsecurityalliance.org/research/working-groups/internet-of-things/.

C.M. (2021, July 14). *Fake delivery bookings will become an actual crime, thanks to new Senate bill*. Https://Ph.News.Yahoo.Com/Fake-Delivery-Bookings-Become-Actual-082128922.Html. Retrieved July 14, 2021, from https://ph.news.yahoo.com/fake-delivery-bookings-become-actual-082128922.html

Crossman, A. (2020, March 19). Understanding Purposive Sampling. Https://Www.Thoughtco.Com/Purposive-Sampling-3026727. Retrieved March 19, 2020, from https://www.thoughtco.com/purposive-sampling-3026727

Cybercrime: A threat to network security - IJCSNS. (n.d.). Retrieved from http://paper.ijcsns.org/07_book/201202/20120214.pdf.

D.D.L.O. (2020, March 3). The Anti-Photo and Video Voyeurism Act of 2009: A Primer. Https://Www.Privacy.Com.Ph/the-Anti-Photo-and-Video-Voyeurism-Act-of-2009-a-Primer/. Retrieved March 3, 2020, from https://www.privacy.com.ph/the-anti-photo-and-video-voyeurism-act-of-2009-a-primer/

(Djanggih et al., 2018) The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia Retrieved from: https://iopscience.iop.org/article/10.1088/1742-6596/1028/1/012192/meta

How to organize a paper: The imrad format. The Visual Communication Guy. (2017, March 12). Retrieved from https://thevisualcommunicationguy.com/writing/how-to-organize-a-paper/how-to-organize-a-paper-the-imrad-format/.

Identity Theft | USAGov. (n.d.). Www.usa.gov. Retrieved March 15, 2022, from https://www.usa.gov/identity-theft?fbclid=IwAR1Z8BCCl0ufAwSCSWWT2R0adnHmrKWErvJMt58eDiONI8bYnUA6uQ0zrCA

Identity Theft. (2015, June 9). Www.justice.gov.

https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud?fbclid=IwAR2Ag2VZFHj57NSTGhbWwS9UgIhM_mQsVfoB1bUHrLBJhhcO_7oFIJbepaA

Identity Theft. (2015, June 9). Www.justice.gov.

https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud fbclid=IwAR2Ag2VZFHj57NSTGhbWwS9UgIhM_mQsVfoB1bUHrLBJhhcO_7oFIJbepaA

INTERPOL. (2020, August 4). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Https://Www.Interpol.Int/En/News-and-Events/News/2020/INTERPOL-Report-Shows-Alarming-Rate-of-Cyberattacks-during-COVID-19. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Jaishankar. (2017). *Space transition theory of cybercrimes*. Research Gate. Retrieved December 7, 2021, from https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes.

Jaishankar, P. (D. K. (2018, April 6). *Space transition theory simplified* R. Rochin Chandra and K. Jaishankar*. LinkedIn. Retrieved December 13, 2021, from https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar.

Jochims, K. (2021, October 5). *Covid-19 and Cybercrime*. Revelock a Feedzai Company. The Cloud Platform to Manage Financial Risk. Retrieved from https://www.revelock.com/en/blog/covid-19-and-cybercrime.

Kansas State University. Phishing and other cybercrime. (2021, September 30). Retrieved January 11, 2022,fromhttps://www.k-state.edu/it/security/protect-yourself/phishing-cybercrime.html#:~:text=scams%20and%20malware.-,Phishing%20scams,you%20to%20a%20fake%20website. e perpetrators Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167404815001844 at/Article/View/6550/5407. Retrieved from https://www.turcomat.org/index.php/turkbilmat/article/view/6550/5407

Manila Standard. (2021, August 12). PNP steps up campaign vs. Cybercrimes, sues 87. Https://Manilastandard.Net/Mobile/Article/362233. Retrieved from https://manilastandard.net/mobile/article/362233

N.D.V.L.O. (2017, May 20). Is the Act of Spreading Nude Photos or Sex Videos in the Internet

Punishable in the Philippines? Https://Ndvlaw.Com/Is-the-Act-of-Spreading-Nude-Photos-or-Sex-Videos-in-the-Internet-Punishable-in-the-Philippines/. Retrieved May 20, 2017, from https://ndvlaw.com/is-the-act-of-spreading-nude-photos-or-sex-videos-in-the-internet-punishable-in-the-philippines/

Katharina.kiener-Manu. (n.d.). *Cybercrime module 3 key issues: The Role of Cybercrime Law*. Cybercrime Module 3 Key Issues:

The Role of Cybercrime Law. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

Konradt C., Schilling A. & Werners B. (2016) Phishing: An economic analysis of cybercrime perpetrators Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167404815001844

Li, J. (2021, May 10). Cybercrime in the Philippines: A Case Study of National Security. Https://Www.Turcomat.Org/Index.Php/Turkbilmat/Article/View/6550/5407. Retrieved from https://www.turcomat.org/index.php/turkbilmat/article/view/6550/5407

Manila Standard. (2021, August 12). PNP steps up campaign vs. Cybercrimes, sues 87. Https://Manilastandard.Net/Mobile/Article/362233. Retrieved from https://manilastandard.net/mobile/article/362233

N.D.V.L.O. (2017, May 20). Is the Act of Spreading Nude Photos or Sex Videos in the Internet Punishable in the Philippines? Https://Ndvlaw.Com/Is-the-Act-of-Spreading-Nude-Photos-or-Sex-Videos-in-the-Internet-Punishable-in-the-Philippines/. Retrieved May 20, 2017, from https://ndvlaw.com/is-the-act-of-spreading-nude-photos-or-sex-videos-in-the-internet-punishable-in-the-philippines/

Nicolas and De Vega Law Offices. (2020, April 20). *Computer-related Identity Theft is a Serious Cyber Crime - Law Firm in Metro Manila, Philippines | Corporate, Family, IP law, and Litigation Lawyers*. Ndvlaw.com.

https://ndvlaw.com/computer-related-identity-theft-is-a-serious-cyber-crime/?fbclid=IwAR0me4F6F3-AinZNZdHJBfpsOmgn71503e3WM6uOKs4gZAHJCgID8MMH30A

NSW Attorney General’s Department. (2011). Routine activity theory crime prevention. Http://Www.Crimeprevention.Nsw.Gov.Au/Documents/Routine_activity_factsheet_nov2014.Pdf. Retrieved 2011, from http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

Pachico, E. (2017, October 6). *'Mexico internet scam extorts applicants for fake jobs'*. InSight Crime. Retrieved January 11, 2022, from https://insightcrime.org/news/brief/mexico-internet-scam-extorts-applicants-for-fake-jobs/

https://neurolrespract.biomedcentral.com/articles/10.1186/s42466-020-00059-z

Pinoy Stack. (2021, April 10). *Fake Booking Cases In The Philippines Is On The Rise*. Https://Pinoystack.Com/Blog/Social-Media/Fake-Booking-Cases-in-the-Philippines-Is-on-the-Rise/.

Retrieved April 10, 2021, from https://pinoystack.com/blog/social-media/fake-booking-cases-in-the-philippines-is-on-the-rise/

PNP Anti-cybercrime Group. (2018). *Common types of internet fraud scams*. Common Types of Internet Fraud Scams. Retrieved March 16, 2022, from https://pnpacg.ph/main/contacts/2-uncategorised/172-common-types-of-internet-fraud-scams.html

Purposive sampling 101: Alchemer blog. Alchemer. (2021, August 26). Retrieved from https://www.alchemer.com/resources/blog/purposive-sampling-101/.

Radoini, A. (2020, March 1). CYBER-CRIME DURING THE COVID-19 PANDEMIC. Http://F3magazine.Unicri.It/?P=2085. Retrieved from http://f3magazine.unicri.it/?p=2085Statista Research Department. (2021, December 1). Number of cyber-crime incidents within the National Capital Region of the Philippines in 2019, by type. Https://Www.Statista.Com/Statistics/1134996/Philippines-Cyber-Crime-Victims-Ncr-by-Type/. Retrieved from https://www.statista.com/statistics/1134996/philippines-cyber-crime-victims-ncr-by-type/

Taguig. PhilAtlas. (n.d.). Retrieved from https://www.philatlas.com/luzon/ncr/taguig.html

Touryalai, H. (2021, January 7). *Countries with the most card fraud: U.S. and Mexico*. Forbes. Retrieved January 11, 2022, from https://www.forbes.com/sites/halahtouryalai/2012/10/22/countries-with-the-most-card-fraud-u-s-and-mexico/?sh=4e780d6c4708

T.L.A.W.P.H.L.P. (2010, February 15). AN ACT DEFINING AND PENALIZING THE CRIME OF PHOTO AND VIDEO VOYEURISM, PRESCRIBING PENALTIES THEREFOR, AND FOR OTHER PURPOSES. Https://Www.Lawphil.Net/Statutes/Repacts/Ra2010/Ra_9995_2010.Html. Retrieved February 15, 2010, from https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html

Tyler, M. (2013, May 23). The Impact of social media in Our Daily Lives. Https://Linguagreca.Com/Blog/2013/05/Impact-of-Social-Media-in-Our-Lives/. Retrieved from https://linguagreca.com/blog/2013/05/impact-of-social-media-in-our-lives/

Types of Identity Theft | Equifax® - United States - Evo Prod. (n.d.). United States. Retrieved

March 15, 2022, from https://www.equifax.com/personal/education/identity-theft/types-of-identity-theft/?fbclid=IwAR2rPDPNNoqZYePnsVj-3iIh5RiysFbWSkwpExYRubjXEokToA3UpVtrLio

Unknown. (2021, August 4). *Interpol report shows alarming rate of cyberattacks during COVID-19*. INTERPOL. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

VanDevanter, N., Combellick, J., Hutchinson, M. K., Phelan, J., Malamud, D., & Shelley, D. (2012, February 16). *A qualitative study of patients' attitudes toward HIV testing in the dental setting*. Nursing Research and Practice. Retrieved from https://www.hindawi.com/journals/nrp/2012/803169/.

(Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? - Fawn T. Ngo, Alex R. Piquero, Jennifer LaPrade, Bao Duong, 2020, 2021)

What is phenomenological qualitative research? Invoke. (2020, July 20). Retrieved from https://invoke.com/blog/what-is-phenomenological-qualitative-research.

Yar, M., & Steinmetz, K. F. (2020). *Cybercrime and society*. MTM.

Zoleta, V. (2022, January 12). *Online scams in the Philippines you need to watch out*. Moneymax. Retrieved March 16, 2022, from https://www.moneymax.ph/personal-finance/articles/online-scams-philippinesemployment_with_the_company