Linguistic Manipulation by Scammer as Cyber Crime: Viewed from Law and Education

Hendrikus Male[1], Erni Murniarti[2], Ronny Gunawan[3], Masda Surti Simatupang[4]
{hendrikus.male@uki.ac.id[1], erni.murniarti@uki.ac.id[2], ronny.gunawan@uki.ac.id[3], masdasimatupang@uki.ac.id[4]}

Universitas Kristen Indonesia, Jl. Mayjen Sutoyo no.2 Cawang-Jakarta 136301234[1234]

Abstract. Cybercrime on emails or other social media is now drawing careful attention to the academics and police. Such issue is not new to the police but it might be new to academics. Many people might be easily cheated on the language used by the scammer when they are influenced by the scammers' manipulation language. This study employed a qualitative analysis. a content analysis is used as the method of the study. The result of the study is that the language used by the scammer is very much convincing. The scammers persuaded and manipulated the language to deceive their victims. It is highly suggested that academics should also pay a careful attention and educate other people by spreading a clear information to their students or doing socialization to the society in community service program. This way can also help the police to reveal the crime spread on cyber world.

Keywords: Language Manipulation; Cyber Crime; Scammer

1 Introduction

Since the internet has now been widely used, the cyber criminals were also find their way to manipulate other people. Yar (2012) [1] showed that the development of new social media was reshaping forms and patters of criminals' victimization in the online environment. Cybercrime committed by cyber criminals or scammers has recently become more prevalent in our society nowadays. It may also become the major threat for all the people who utilize the internet. Many reasons are done by scammers to deceive their potential victims. The victims were promised a large amount of funds in the form of parcels. They also use convincing expressions that victims might fall into their traps.

Another study conducted by Iswara and Bisena [2] said that fake news makers on digital media use the language as the instrument to manipulate facts and produce lies. If this is the first time, the prospective victims are tempted by the promised time. In their actions, they use disguises as well-known figures such as famous diplomats. They also use foreign phone numbers to carry out their plan of action. this way is believed to assure their targeted victims.

Cybercrime committed by scammers has become a serious problem for everyone who uses social media such as WhatsApp, emails, and others when accessing the internet. Scammers are people who do the fraud or take part in dishonest activities like cheating good people for their personal benefits. According to online Cambridge Dictionary [3] scammer means someone who makes money using illegal methods, especially by tricking people. It is obvious that the sense of scammer is negative. Wadi and Ahmed [4] said when scrutinizing

ICLHR 2021, April 14-15, Jakarta, Indonesia

DOI 10.4108/eai.14-4-2021.2312842

text in in media critically, it deals with the role of discourse (language in use). In their action, the cyber criminals can outsmart their prey using convincing expressions of language. They make use any effort to reassure their potential victim.

To interact or communicate verbally and in writing, people use language as the medium. Language is used in all disciplines of knowledge including law. Policymakers make rules using language, lawyers use language to communicate, and make rules to provide protection to the accused. This is regulated in the laws or constitution governing a country. Studying the field of law has always been a very interesting field for languages because they cannot be separated from one another. If it is with language manipulation, the victims are usually not aware that they are being trapped.

It is believed that reassuring other people to believe in what one may do is considered as manipulating in the form of motivating, insistence, convincing. Asya [5] pointed out that in psychology the term "manipulation" is defined as type of psychological affection, which in case of skilful realization leads to implicit provocation of another person's intentions that do not correspond to his actual wishes and his stimulation towards commitment of actions required by the manipulator. When it deals with social media, it cannot be separated from the language use in the media. Some use it very convincing, some other use it provocatively. Paltridge [6] suggested that text is inseparable from social reality. Wadi and Ahmed [7] in their study found out that the media messages are not as neutral as they claim to be. They went on mentioning that language has and still plays a crucial role in framing and shaping.

2 Literature Review

In simple terms, linguistic manipulation can be defined as the activity of engineering a language to achieve a goal. Whereas more broadly, manipulation is essentially a process of deliberate engineering by adding, hiding, removing, or obscuring parts or all of a source of information, substance, reality, reality, facts, data, or history made based on the design system. which can be done individually, in groups, or in a value system. Manipulation is an important part of a particular goal in terms of the act of planting ideas, dogmas, doctrines, attitudes, systems of thought, behaviour, and certain beliefs [8]. This is in line with Asya [9] stating that linguistic manipulation in a broad sense is any verbal interaction regarded from the point of view of its motivation and realized by the subject (speaker) and the object (listener) of communication.

Lewandowski [10] states that language manipulation is an action to influence or direct the behaviour, attitudes, and opinions of others by using language. Darmojuwono [11] shows that language manipulation can be done in various ways, including:

a. Using words that contain elements of emotive meaning can lead to positive or negative emotions.
b. Using words that are ambiguous/unclear to allow for the expansion/refinement of the concept according to purpose
c. Blurring the concept of words through euphemisms
d. Using metaphors as an indirect way of revealing the reality

As previously explained, language manipulation is an engineering activity in the field of language. The manipulation is mostly done through the cyberspace. Cyberspace offers up many benefits, but many more substantial risks [12]. By the Engineering activities in the context of their use can have both positive and negative aims.

However, in this study, the language manipulation activities found were negative language manipulation engineering. Therefore, the purpose of using language manipulation is used to deceive many people via email. The victims were promised a large amount of funds in the form of parcels. They also use convincing expressions that victims fall into their traps. If this is the first time the prospective victims are tempted by the promised time. In their actions, they use disguises as well-known figures such as famous diplomats. They also use foreign phone numbers to carry out their plan of action.

2.1 Cybercrime

There is a fast range of motivations and knowledge among cybercriminals, and the ways of expressing these are many and varied [13]. Crime in cyberspace can be interpreted as a computer crime. Crime in cyberspace according to [14], The U.S department of justice defines a computer crime which is defined as: ... any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution. According to the Organization of European Community Development [15] Cybercrime is all forms of illegal access to data transmission. This means that actions that are not legal in a computer system are included in a crime. One of the examples of crime is deception.

Rusmana [16] stated that deception is an act a person or group of people makes an impression that something is true and not fake to make other people trust. Another problem of cybercrime is hacking that has become a weapon. Many kinds of people can hack into critical information infrastructure, such as criminals who want to blackmail the owner of a system, terrorist groups, or even mercenaries or government agencies wanting to generate chaos in another country through cyberspace [17]. In general, cybercrime can be defined as an act of crime in cyberspace that utilizes computer technology and internet networks as targets.

Types of cybercrimes [18]

1. DDoS Attacks: These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.
2. Botnets: Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.
3. Identity Theft: This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.
4. Cyberstalking: This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically, cyberstalks use social media, websites and search engines to intimidate a user and instil fear. Usually, the cyberstalked knows their victim and makes the person feel afraid or concerned for their safety.
5. Social engineering: Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find

out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

6. PUPS: PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it’s a good idea to install an antivirus software to avoid the malicious download.
7. Phishing: This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.
8. Prohibited/Illegal content: This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.
9. Online scams: These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information.
10. Exploit kits: Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user’s computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

A study conducted by Aryyaguna [19] reported that there were some problems encountered by the police such as the aspect of investigator in terms of their level of ability and skill, evidence in terms of data is vulnerable to change and remove, facilities in terms of computer forensic laboratories and jurisdiction. In addition, crime in cyberspace is increasingly prevalent today. It is not only done publicly but also by using manipulation language with the aim of convincing and even threatening potential victims in order to submit and obey to the criminals. Recently, the crimes committed by fraudsters in cyberspace have been fraudulent using social media, such as Facebook, WhatsApp, YouTube, Emails, and others. Following are the crimes on social media that are often committed by scammers, including phishing, scams, faking someone's Facebook account, and others.

Phishing is a crime that is committed via email, telephone, or a link that goes to an email. The way the scammers work is very neat and certainly not at all suspicious of ordinary people who do not really understand cyberspace. Furthermore, fraudsters who are phishing usually work in groups to carry out their actions. They will not be responsible for making other institutions such as shipping services, banks, and other related institutions with a website that seems official. This study focuses on phishing or scam on email. Scammers or criminals who are done on emails are better known as scammers. The scammers who do this language manipulation are very good at using language for their own purposes. The writers therefore, are interested to do the research and to find the linguistics manipulation as well as viewed from the aspects of law and education

3 Research Methods

This research is qualitative research. This research on language manipulation in an email was carried out in three stages, namely the data collection stage, the data analysis stage, and the data presentation stage. Data obtained through observation, while the technique used is documentation. Subsequent data is presented in formal and informal forms. This study employed the critical discourse analysis [20] and reported a content (text) analysis from emails taken from an-almost victim of fraud. For the sake of security. All the names would not appear in this study and not all of the text conversation were scrutinized. It merely discussed the linguistic manipulation and also viewed from the law and education aspects.

4 Results and Discussion

The first research questions of this study is to find out the most dominant linguistics manipulation and followed by the linguistics manipulation viewed from law and education. In this study the discussion merely focused on linguistic manipulation in the sense of the use of euphemism, positive or negative emotion that are considered and categorized as the manipulation in language. In addition, the extracts that are taken from the conversation in emails are not scrutinized all. It only discussed the situation which the scammer manipulated the prey.

The following are the extracts taken from an email.

(Extract≠1)

The Scammer: *Hello! I apologize if this email comes as a surprise to you. I had to reach out to you through your email because I have something of great importance I would like to divulge for further discussion. Please kindly let me know if we can talk further on this note. Best regards,sir ...*

The almost victim: *Hi sir what can I do to help you?*

In the first introduction the scammer greeted and apologized. This is believed as an attempt to manipulate the- almost victim to believe of the scammer's language manipulation.

Next extract: (Extract≠2)

The scammer: *I hope you are doing great. I know you will be surprised to see my message because we hardly know each other but I have summoned up courage to contact you*. (Extract≠ 1)

It is obvious that the scammer admitted that they hardly knew each other but he had summoned up courage to contact the 'an-almost victim' although he started it politely by hoping that his victim had a great day. From this extract, the scammer started to manipulate the victim by convincing himself that he had the courage to contact. The scammer also tried to blur the idea using euphemism by pretending to ask the situation and condition 'I hope you are doing great'.

The next extract (Extract≠3)

The scammer: *My Name is Sir ... from the United Kingdom. I'm presently British Ambassador to the European Union and want to venture into private investments. I want to invest in real estate or any other profitable businesses. I decided to contact you to assist me in managing my investment portfolio in your country since I will not always be there for the day to day running of the business because I'm still active with some governmental appointments.*

The above extracts show that the scammer outsmarted the almost victim by introducing himself as a well-known public figure, an ambassador and from the UK. He also told the almost victim to venture into private investments. From the extract, it is also scrutinized that why the scammer did not invest his money legally involving the government or other party to run his business. In fact, he already lied to the almost victim. It is also suspected that the scammer did not want to invest his money legally.

Extract (Extract≠4)

The scammer: *I made the sum of (GBP 11,380,000) in an Oil deal I did with some… citizens while I was serving in ... and now, I want to move this Fund somewhere and invest it. For your humble assistance, I will give you 20% of the money which is (Two Million, Two Hundred and Seventy Six Thousand Pounds Sterling) as i do not want to lose my money to the security company because i have worked so hard to safeguard it for the past years.*

The above extract shows that the scammer promised to give a huge amount of money if the-almost victim could assist him.

Extract (Extract≠5)

The scammer: *I want you to bear in mind that I meant well for us and would like us to trust and co-operate with each other so that we can finish the transaction successfully. There is no risk involved. Every arrangement to move the money has been taken care of.*

From the above extract, it can be seen that the scammer again attempted to convince the almost victim to trust and could cooperate with each other. He also convinced the almost victim if there was no risk. It is also believed that the scammer knew how to outsmart the almost victim.

Extract (Extracts≠6)

The scammer: *Considering my status as a ... Ambassador to the European Union, I cannot be able to do much from here, that's the main reason I want you to handle this transaction on my behalf. It's better I give you that amount than losing the whole money to the company, so do not be worried because I have all the documents to back up the source of the fund and with these documents you can deposit the fund in any bank in the world and no government authority will question you.*

The scammer*: I already receive message from the UN to forward the account details to me so i can send to you to make the payment immediately. I will forward to your email shortly. Kindly make the payment immediately so you will receive the consignment without delay.*

The-almost victim: *Sir can I pay after I get the luggage?*

The Scammer: *They said you have to make the payment before can release the consignment. I got a message from the UN courier that you have to pay RP9.500.000. You have to make the payment immediately so you can receive the consignment without further delay. Can i send the account info here or in your email? You have to make the payment now so that you will receive the consignment without delay.*

The-almost victim: *here is fine. By the way sir, according to Indonesian law, any imported things should have the tax. And the tax should be paid to the government. With the government official account.*

The scammer: *No you just don't get it. It is safer and more secured to send through diplomatic courier to avoid interrogation from bank Indonesia and other securities.*

The –almost victim: *I see*

From the conversation text above (Extracts≠6), it is obvious that the scammer fabricated and admitted to already have message from the fake UN Courier to deceive their prey. It does not make any sense at all. How could he invest his funds in other country without any tax payment to the targeted country? It is illegal and fake. Besides, the consignment (the funds) could be released if the-almost victim had to pay some payment. It has been suspicious by the-almost victim since the scammer rejected to pay the tax to the government.

In terms of linguistic manipulation, the study has revealed that the cybercriminal or scammer used convincing expressions or utterances in doing his action. He also used much effort to reassure his prey. However, the almost-victim was suspicious with all the works and actions conducted. The next discussion is dealing with the law's view regarding the cyber-crime.

According to Indonesian law number 19-year 2016 regarding the information and electronic transaction [21], those who committed crime in any form are considered as criminal and should pay for the penalty as a return for their deceptions or sent to jail. This is done due to the fraudster has committed harm to other parties. For the past few decades, the OECD has also attempted to fight against the cybercrime. In the real field, the police might have a number of obstacles. In order to prevent the crimes, Sirenden [22] in his study, he offered a number of preventive efforts such as carrying out activities outreach to the community, fostering the younger generation, and providing appeals through the media, and repressive measures, namely in the form of means of imposing sanctions or penalties against the perpetrators of fraud to provide a deterrent effect. Therefore, in order to maintain the peaceful life in the society.

The law should be enforced. This in line with Soekanto [23] who affirmed that law enforcement is an activity to harmonize the relationship of values which are translated into solid rules and actions as a series of value translation the final stage, to create, maintain and maintain peace in social life. Additionally, in order to build the security and trust in cyber space, it is suggested that the policy makers who control the information and technology system specifically the cyber security system in our country may consider the cyber security program as follows 1) a national strategy, 2) collaboration between government and industry, 3) a sound legal foundation to deter cyber-crime, 4) a national incident management capability, and 5) a national awareness of the importance of cyber-crime [19]. The motive and causes of why the cyber criminals committed crime should also be further examined [24]

Concerning the education aspect, teachers or lecturers are to educate the students and do a huge socialization to the society in the form of community service. The teachers can also socialize to their students in the class to be careful and not even to respond to the scam on their suspected emails. Criminals who committed this can be assumed by several factors that make them do this, usually because of economic problems. The desire to get money or wealth by shortcut in an illegal way. Education must be carried out in the form of socialization through social media on a large scale to everyone in order to understand that what is done by criminals in cyberspace is an act that violates laws, norms, and rules in society and the country.

Starting from the university level, lecturers specifically who teach information and technology to provide understanding to their students as programmers or technicians to play an active role in helping the police/government in combating crime in cyberspace. Teachers are also hoped to guide the students in terms of making the students aware of to do and not to do on cyber for example by not clicking on unfamiliar links, ads, or suspicious emails. This way is to help the students to use their social media wisely. They are not supposed to reply on scams or phishing or any kind of crimes on social media and not to respond for the suspected or unnecessary information.

4 Conclusion

Scammers or criminals know their best to cheat other people. They seem to be very clever to use their strategies only to get rich in a short cut. As the academics, we have to take time to think it over before deciding to reply the scammer request. We must not compromise with the criminals. Next it is hoped that when doing the online shopping or just surfing the internet, we are suggested to never pay upfront for goods that we never received yet. They do not even give their prey to think for there are good at manipulating others. It is concluded that to avoid being deceived by the cyber criminals like scammers. The educators and the police should collaborate to find out the solution together for example doing the socialization on social media as much as possible or doing the socialization in a community service program. This study found out the linguistic manipulation used by the cyber criminals or scammers are very convincing and insistence to outsmart their prey.

Suggestion

The cyber criminals usually target the inexperienced people to become their prey. The security system of cyber should also be strengthened legally. It is suggested not to easily believe any incoming emails or scams instead taking extra precautions to protect from deception or theft on personal data. Due to some limitations and time constraint, it is suggested that the future research can be done in the same area of study

References

[1] Yar, M. E-Crime 2.0: the criminological landscape of new social media. Information & Communications Technology Law, 207-219. (2012).

[2] Iswara, A. A., & Bisena, K. A. Manipulation And Persuasion Through Language Features In Fake News. RETORIKA: Jurnal Ilmu Bahasa, 6(1), 26-32. (2020).

[3] https://dictionary.cambridge.org/dictionary/english/scammer. Retrieved from https://dictionary.cambridge.org/dictionary/english/scammer: https://dictionary.cambridge.org/ (2021).

[4] Wadi, S. I., & Ahmed, A. A.: Language manipulation in media. International Journal on Studies in English Language and Literature, 3(7), 16-26. (2015).

[5] Asya, A.: Linguistic manipulation: Definition and types. International Journal of Cognitive Research in science, engineering and education, 1(2). (2013).

[6] Paltridge, B.: Discourse Analysis. Sydney: University Publishing Services. (2006).

[7] Wadi, S. I., & Ahmed, A. A.: Language manipulation in media. International Journal on Studies in English Language and Literature, 3(7), 16-26. (2015).

[8] https://id.wikipedia.org/wiki/Manipulasi. Retrieved from https://id.wikipedia.org/wiki/Manipulasi: https://id.wikipedia.org/wiki/.(2021, Maret 17).

[9] Asya, A.: Linguistic manipulation: Definition and types. International Journal of Cognitive Research in science, engineering and education, 1(2). (2013).

[10] Lewandowski, T.: Linguistisches woterbuch. Heidelberg: Quelle & Meyer. (1985).

[11] Darmojuwono, S.: Manipulasi bahasa dan prasangka sosial dalam komunikasi. WACANA, 2(1), 32-39. (2000).

[12] Gillam, L., & Vertapetiance, A. (2012). Cyber law, cyber ethics and online gambling. In A. Dudley, J. Braman, & G. Vincenti, Investigating cyber law and cyber ethics (pp. 78-99). Information Science Reference.

[13] Ghernaouti, S. Cyber Power: Crime Conflict and Security in Cyberspace. Lausanne: EPFL Press. (2013).

[14] https://divhubinter.polri.go.id/dhi/viewBerita.php?id=13. Retrieved from https://divhubinter.polri.go.id/dhi/viewBerita.php?id=13. (2021).Computer-related criminality: Analysis of Legal Politics in the OECD Area. (1986).

[15] Rusmana, A.: Penipuan dalam Interaksi melalui Media Sosial: Kasus Peristiwa Penipuan melalui Media sosial dalam Masyarakat Berjejaring. Jurbal Kajian Informasi & Perpustakaan, 3(2), 187-194. (2015).

[16] Ghernaouti, S. Cyber Power: Crime Conflict and Security in Cyberspace. Lausanne: EPFL Press. (2013).

[17] https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/. Retrieved from https://www.pandasecurity.com (2021).

[18] Aryyaguna, A. D.:Tinjauan Kriminologis terhadap Kejahatan Penipuan Berbasis Online: Studi kasus Unit Cyber Crime Reskrimsus Polda Sulsel. Unpblished Undergraduate Thesis. (2017).

[19] Rogers, R.:An Introduction to critical discourse analysis in education. In R. Rogers , An Introduction to critical discourse analysis in education. London: Lawrence Erlbaum Assiciates, Inc. (pp. 1-18). (2004).

[20] Undang-Undang Republik Indonesia nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. (2016).

[21] Sirenden, N.: Tinjauan Kriminologis terhadap Kejahatan Penipuan dengan Modus Undian Berhadiah: Studi Kasus di Kabupaten Sidrap Tahun 2013-2016. Makassar: Unpblished Undergraduate Thesis. (2017).

[22] Soekanto, S.: Pokok-pokok Sosiologi Hukum. Jakarta: Rajawali Press. (1980).

[23] Ennis, J. Best practice for organizing national cyber security efforts' presentation made at regional workshop organized by the ITU in collaboration with ictQATAR and Q-CERT. (2008).

[24] Noble, W. Cyber Armies – The Growth of the Cyber Defence Industry. In T. Owen, W. Noble, & F. C. Speed, New Perspectives on Cybercrime (pp. 63-78). Preston, UK: Palgrave Macmillan. (2017).