Jurnal HUKUM dan KENOTARIATAN

Volume 7 Issue 1, 2023
P-ISSN: 2549-3361, E-ISSN: 2655-7789


# Criminal Implementation Against Cyber Actors Crime Phising

**Vicha Kartika[1], Budi Sastra Panjaitan[2]**

[1]*Faculty of Sharia and Law, State Islamic University of North Sumatra,*
*Email :* vichakartika23@gmail.com
[2]*Faculty of Sharia and Law, State Islamic University of North Sumatra*
*Email :* budisastrapanjaitan@gmail.com

***Abstract :*** *Indonesia is getting more and more advanced day by day, including in the field of electronics. One of the electronic devices is a computer. Many people use computers in their daily activities, which are growing rapidly. Apart from these activities, there are various cases of internet abuse that have become very widespread, ranging from fraudulent fraud, online fraud, defamation, etc. With the ratification of Law no. 11 of 2008 concerning information and electronic transactions jo. Article 27 paragraph (3) Law no. 11 of 2008, so the regulation on the use of information and electronic transactions has received legal action. With this law, crimes in the form of cyberspace (cyber crime) become easier to be legally processed, in cases of cyber crimes it becomes easier, especially in the form of phishing.*
**Keywords**: *Indonesia, Internet, Electronics*

## 1. Introduction

The development of the times in Indonesia is increasingly sophisticated, where one of them is in the field Electronic. The electronic device is a computer, when it was first discovered computer is just a big machine with limited capabilities, devices have experienced major development in both performance and size in a short period of time. Lots of insiders various daily activities have been using the computer, it is also growing rapidly with the invention of the internet in 1969 and a quarter century later. This development of the internet wider and has a variety of benefits, not only the benefits but also the impact loss. More and more use of internet facilities, on the other hand there are various electronic transactions or transactions via online increased from various sectors, which then gave rise to various terms; e banking, e-commerce, e-trade, e-business, e-government, e-education and e-retailing. So far along the course of time is increasing both technology and its use, bringing many good effects positive or negative. Of course in positive terms, we can be grateful for this technology offers many benefits and conveniences. There is no denying that internet technology has many negative effects. Thanks to the internet, traditional crime has developed become a modern crime with a higher loss rate and greater impact.

Because of the large number of internet users in our country, so that the number of internet users is increasing in an information and social medium, there is no possibility of "ideaism" within Indonesia in using Iinteirneit. Various cases of misuse of intelligence have become very widespread, starting from fraud fraud, breach of privacy, online fraud , defamation of good name , etc. If it's too late , how many this case points to one thing, namely the beauty of the digital literacy of Indonesian society . Nope It is known how many phishiing attacks have been launched as cyber crimes . Because performance

continues to generate new ideas to disrupt the activities of the Intelligence. Unfortunately, every year there are more and more cases like this , and intelligence victims cannot be counted with just one finger. Meireika make money the easy way. But they don't always do it for money.

Usually they just want to browse or peek at the activity of the account owner . So far as it is one of the cases mentioned is regarding the defamation of good name which is related to violation of law and misuse of intelligence, one of Siibeir's crimes is against phiisiing. Phiishiing is a form of activity that has the character of threatening or trapping someone with the concept of embracing the people involved. That is, by deceiving someone so that person indirectly provides all the information needed by the investigator. Source The sources of phishiing threats are eimail, weibsiitei, and malwarei.

Phisiing is a form of activity that has the character of threatening or trapping someone with the concept of embracing the people involved. Namely by deceiving someone so that the person is said Mia Haryati Wibowo and Nur Fatimah, "Phishing Threats Against Social Media Users in the World of Cyber Crime," Phishing Threats Against Social Media Users in the World of Cyber Crime 1 (2017): 5. indirectly providing all the information needed by the investigator .

Where now it is rife that criminal acts occur through computer networks . In the social mediation , a case occurred defamation of good names , hate speech and spreading hoaxes. Not to mention the spread of the computer virus, hacking, cardiing, gambling , child pornography and others that are included in cyber crime criimei). So, want to commit criminal acts of defamation , utterances of deceit and spread of hoaxes which is regulated in the Criminal Code (KUHP), UU no. 11 of 2008 concerning Electronic Information and Electronic Transactions (UU IiTEi), as amended by Law No. 19 of 2016, UU no. 40 of 2008 concerning the elimination of racial and ethnic discrimination.

Based on the background above , the formulation of the problem obtained is:

1.How is the crime of phisiing regulated in Indonesian criminal law ?

2.How is the application of law to the crime of phisiing in the Neigeirii court decision? Meidan No. 3006/Piid.sus/2017/PN.Mdn?

## 2. Method

The type of analysis used in this study is normative legal analysis , namely the type of legal analysis obtained from library research , focusing on examining the decisions of the Meiji District Court and on sentencing in order to find out the balance of the judge's decision in deciding the case in question. . By analyzing a legal issue through legislation , literature and other revision materials .

## 3. Criminal Law Arrangements in Indonesia Against Cyber Crime in the Form of Phishing

In the Indonesian constitution , it is contained in the Book of the Criminal Code (KUHP) which contains articles that can be applied to cyber crime. Usually these articles are used in more than one article because they involve several actions at once. Of course, the behavior of cybercriminals in the form of phishing that is circulating in cyberspace

must be subject to sanctions in the form of criminal responsibility for the mistake he has made. As stated in the IITEI Law , as well as the regulations of Indonesian law enforcement that regulate crimes by using electronic media or cybercrimes , which use the form of punishment in the form of prison sentences and/or fines in order to be able to find out whether a conviction or a penalty is imposed i share the phisiing behavior that is included in it , has been effective in reducing balanced crime as well as reducing the reciprocity of the behavior itself or not .[1]

Punishments and laws assigned to phishing behavior Law Number 11 of 2008 on Internet and Electronic Transactions (ITE) : :

1. Article 27 of Law I TE of 2008
2. Article 28 of Law I TE of 2008
3. Article 29 of Law I TE of 2008
4. Article 30 of Law I TE of 2008
5. Article 33 Law I TE Year 2008
6. Article 34 Law I TE Year 2008
7. Article 35 Law I TE Year 2008[2]

Using Criminal Law Clauses in Sentences In cybercrime cases , it is only carried out on the basis of intelligence, because there is a distinction between the types of cyber crime and existing conventional crimes, while the method of fraudulent phiishiing and the idea of the Criminal Code have the same elements in the act of will but still there are differences from the beginning to the end . Judging from the form of the crime , the idea of the suspect's identification has reached the rhythm of the crime. Therefore , cyber crime is a relatively new group of crime types , similar to cyber crime following the balance of new technology .

This makes it necessary to clarify specific rules for dealing with the criminal behavior of cybercrime. Because if we only depend on separate interpretations , it creates conflicts of legal consistency in the practice of enforcing weak law . Remember , this also relates to the principle of legality, that is , no action can be punished except according to criminal law , before being threatened with imprisonment because this will humiliate i Cybeircriimei know far adopted by the whole society before rule.

Regarding its interpretation, Andii Hamza stated that legal interpretation is divided into 5 (five) types of interpretation, including:

1. Grammatical interpretation , namely the interpretation of every word in a law.
2. Systematic interpretation , namely the interpretation of the relationship in a criminal law as a whole general.
3. Historical interpretation , namely the interpretation of the intent of the legislator when it comes to ethics the said law was created.

---

[1] Leticia M. Malunsenge, Cornelis Dj. Massie, and Ronald E. Rorie, "Law Enforcement Against Perpetrators and Victims of Cyber Crime in the Form of Phishing in Indonesia" (2009).

[2] Budi Suharto and Arnold Bagas Kurniawan, "Cybercrime Crime for Perpetrators of Falsification of Data on E-Commerce (Phising) Sites," *JHP 17 (Journal of Research Results)* 5, no. 2 (2020): 57–61, http://jurnal.untag-sby.ac.id/index.php/jhp17.

4. Theological interpretation , namely the interpretation of the purpose of a law.
5. Elective interpretation , in which this interpretation is carried out by broadening the meaning of a keiteintuan.3

The legal structure of cyber crimes in the form of phishing was previously regulated in Article 378 of the Criminal Code on fraud, because it is clear that phishing is basically an act of fraud. Fraud as meant in Article 378 of the Criminal Code is:

> "Anyone who with the intention of obtaining unauthorized benefits for himself or another person , with the intention of using a false name or reputation , with deception or a series of lies , provokes another person , steals goods or other goods, or confesses or cancels a debt, because this fraud can be punished law imprisonment for up to four years."

How many elements are contained in Article 378 of the Criminal Code

1. Anyone
2. With the intention of benefiting oneself or someone else
3. Against the law
4. Using a pseudonym or false prestige . By deceiving or lying
5. Motivating others
6. Giving something to him, incurring debt or canceling claims.

Prison is a popular type of punishment in Indonesia, and is frequently used by judges in trials, even for all types of crimes . Judging from the formulation of the mandatory punishment for prison terms , this is a legacy from the classical school which imposes fixed sentences . However, Barda Nawawii Ariif believes that the consequences of being in prison are not only in the form of deprivation of freedom, but also in negative effects, even the perpetrators of crimes will become even more evil after leaving prison.

Later, Muradii added in his book Criminal Justice Systems Kapiita Seileikta (1992) that the consequences of imprisonment can degrade human dignity, that detention is risky and can cause " crime stigma".

Meanwhile, if you look at it based on the characteristics of the Obstruction of Justice act, as explained by Keindall, who stated that the said act or attempt was declared a criminal act that obstructed the legal process , if it fulfills 3 (three)important elements , namely:

a. This action caused delays in legal proceedings (peindiing judicial proceedings);
b. Behavior knowing about his actions or being aware of his actions (knowledgei of peindiing proceedings);

[3] Dion Valerian, *Application of Analogies in Indonesian Criminal Law* (Yogyakarta: Ruas Media, 2017).

c. The behavior commits or attempts acts that deviate from the goal of disrupting or interfering with legal proceedings or administration (acting corruptly with intent).[4]

With the passing of Law No. 11 of 2008 concerning Information and Technology and Electronics (UU IiTEi) on April 21, 2008, regulations concerning the use of information and electronic transactions have received legal action. With this Law , crimes in the form of cyberspace (cybeir crime) are becoming easier to process legally because actions or electronic information , electronic documents and their printed output are a legal means of legal evidence , thus proving in cases of Cybercrime crime . become more easily especially in the form of Phiisiing.

Determine who the person is. Well, that 's the behavior that committed the Criminal Fraud .

There is an intention to benefit oneself and others , meaning that this intention is carried out as a sign. Apart from that, this act is illegal, meaning that the fraudulent person does not have the right to gain any profit as a result of the said fraud . The same is the case with the Neigeirii Meidan Court decision No. 3006/Piid.sus/2017/ PN.Mdn with the case of committing a crime " intentionally and without rights to distribute and make access to electronic information and electronic documents containing insulting and defaming content " as regulated and punishable by law in Article 45 verses (3) UURIi No. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Electronic Information and Electronic Transactions jo. Article 27 paragraph (3) of Law no. 11 of 2008 concerning Electronic Information and Electronic Transactions. [5]_

Defaming someone's reputation in this context is not sexual in nature in the sense that insulting someone 's reputation with slander or humiliation usually damages someone 's reputation . This sense of honor is objectified in such a way that it has to be observed through specific behaviors whether a person in general feels offended or not. It can also be said that children are not yet able to experience this kind of violation , so is the most insane person . The provisions for humiliating the President as Head of State are regulated in the Criminal Code (KUHP), namely in CHAPTER III Crimes Against the Dignity of the President and Deputy President, in Article 134 namely intentional humiliation of the President or Deputy President of the Republic of Indonesia. law with imprisonment for a maximum of six years or a maximum fine of Rp. 4,500.-. And Article 136, the policy that the statement of intentional intentional humiliation in Article 134 also includes the actions described in Article 315, if this is done if the person being insulted is not present, that is, either in public with several actions, or not in public, but in the presence of more than four people or in front of other people , who are present with their unwillingness and who feel their hearts are touched , that is, with actions, or with speech or with writing.

[4] Asrullah Dimas, Muh Hasrul, and Hijrah Adhyanti Mirzana, "Legal Protection of Advocates for Interpretation of Obstruction of Justice" 5 (2021).

[5] Sahrul Mauludi, *Beware of Hoaxes: Smart in Dealing with Defamation, Hate Speech and Hoaxes* .

Article 137 stipulates that: (1) Whoever broadcasts, shows or displays writing or pictures whose contents wish the President or Deputy President's contents to be known by the public or the Deputy President with the intention that the contents of which want to be known by the public or better known by the public, shall be punished with imprisonment for life. one year four months or a maximum fine of IDR 4,500.

(2) If the person commits the crime in his office and at the time of committing the crime it is not yet two years after his previous sentence was fixed for a similar crime , then he can be dismissed from his office . So, the increasing number of activities that are utilized by the internet , resulting in an increase in the number of internet users throughout the world. Therefore , in line with the development, progress and balance of information technology through intelligence, human civilization is faced with new phenomena that are capable of changing almost every aspect of human life [6]

## 4. Application of Law Against Phishing Crimes in the Medan District Court Decision No. 3006/Pid.sus/2017/PN.Mdn

Before the IiTEI law was passed, cybercrime cases in Indonesia were tried by analogy using articles that are in line with the elements of criminal law, so that the punishment for perpetrators of cybercrime uses criminal law or the Criminal Code. In the perspective of crimiinology there are several factors and motives that led to the occurrence of cybercrime crime cases . Based on the motives that occurred, cybercrime crimes can usually be classified into 2 classifications, namely:

1) Criminal intellectual motives that are carried out only as personal satisfaction as well as demonstrating that if they are already able to carry out engineering as well as implementing information technology sectors . Crimes with this motive are usually carried out by someone with an individual conscience .
2) Economic, political, as well as criminal motives implemented as personal profit / certain special groups
3) whose impact is to the economic and political losses of other parties . Because it has a hugely effective purpose , crimes with these motives are usually carried out by a corporation..[7]

As a network in a computer that can be distributed throughout the world, iinteirneit is referred to as a transportation route for all information in the form of files or data on other computers. In the social mediation, there were cases of defamation , utterances of dishonesty and spreading of hoaxes. The cybercrime crime in the form of phisheding uses the IiTEi Law, because punishment under the IiTEi Law uses a combination of cumulative and alternative systems, in which the judge must choose between only imprisonment, fines only, or both to determine the sentence. at the same time.

Because of this it is related to the verdict of the Neigeirii Meidan District Court No. 3006/Piid.sus/2017/PN.Mdn stated that the defendant Muhammad Farhan Balatiif Aliias

[6] Soesilo R, *Book of Criminal Law* , Bogor. (Politeia, 1995).

[7] Akbar Galih Hariyono and Frans Simangunsong, "LEGAL PROTECTION OF VICTIMS OF PERSONAL DATA THEFT (PHISHING CYBERCRIME) IN A CRIMINOLOGICAL PERSPECTIVE" (nd).

Riinggo Abdiillah had been legally proven and convinced that he was guilty of committing a crime under the IiTEi Law . The defendant committed the act of phishing or by asking the owner of the Facebook account to provide information and passwords for the user who owned the Facebook account by sending a link containing the quiz.

The public prosecutor handed down a sentence against the defendant Muhammad Farhan Balatiif Aliias Riinggo Abdiillah with a prison term of 2 years in prison reduced for as long as the accused is in interim detention while the order for the accused remains in detention and a fine of Rp. 10,000,000.- (ten million rupiah) subsidiary of 3 months imprisonment. Meanwhile, the Meidan District Court of Justice (PN) chaired by Wahyu Praseityo Wiibowo, sentenced Farhan to 1 year and 6 months in prison . Farhan wasalso sentenced to Rp . 10,000,000.- (ten million rupiah) subsidiary of 1 month in prison.

The prosecutor following indictments accused Muhammad Farhan Balati (alias i Abdi ) :

Main Charges: Violation of Article 46(3) jo Article 30(3) RIi. Amendment to Law No. 19 of 2016 to become Law RIi No. 11 of 2008 concerning Information Technology and Electronic Transactions. Title 11 of 208 is related to electronic information and transactions .

Subsidiary: Violation of Variation of Law No. 19 of 2016, Article 45(2) UU RIi. Article 28(2) RIi Law No. 11 of 2008 concerning Information and Electronic Transactions Law no. 11 of 2008 concerning Electronic Information and Transactions .

Leibiih Subsiideir: Violation of Article 45(3) UU RIi. Amendments to Law No. 19 of 2016. Article 11 Paragraph 27(3) RIi Law No. 11 of 2008 concerning Electronic Information and Electronic Transactions Decree No. 11 of 2008 concerning Electronic Information and Transactions .

According to the researcher, the indictment filed by the public prosecutor is in accordance with the chronological order of the crime of defamation of social media , because in the main indictment, the subsidiary or more subsidiaries have fulfilled the requirements in the said article. The judge also decides which of the charges he chooses has been proven and is free to state that the main charges have been proven without prior decision on the charges, subsidiary charges and subsequent subsidiary charges. That is, if one of the charges has been proven, then the other charges do not need to be proven again.

In its verdict, the panel of judges considered that based on the results of the trial at trial, Farhan had been proven legally and convincingly guilty, because he committed the crime deliberately and without the right to distribute, making it possible to access electronic information that has a content of insults as a whole irta respects the good name of Preisiidein Joko Wiidodo and Kapolrii General Tiito Karnaviian. In that it is also stated, considering that in order to impose a sentence on the Defendant, it is necessary to consider in advance the circumstances that are aggravating and facilitating the defendant. Impressive circumstance

1. The actions of the Defendant caused damage to the good name of the Head of State of the Republic of Indonesia
2. The actions of the Defendant caused harm to the Indonesian Republic of Indonesia 's Police Institutions and Kapolrii as the leader of the Highest Level of the Republic of Indonesia's Police
3. The actions of the Defendant may cause hatred in society towards the Head of State.

Favorable circumstances :

1. The defendant regretted and admitted his actions

2. The defendant promised not to repeat his crime again

3. The defendant was still young and had the opportunity to change better

4. The defendant and the defendant 's family have apologized through social or electronic media

Because of that , the defendant was found guilty and convicted , so the defendant was also burdened with paying court fees . Based on the facts of the case , which were revealed in the trial, namely the testimony of the witnesses including the accused's biases in accordance with each other , coupled with the existence

of such valid evidence , it can be concluded that all elements of the prosecutor's indictment have been complied with. From the judge's decision it can also be concluded that the defendant was sentenced to a prison term of 1 (one) year 6 (eix) months and a fine of Rp. 10,000,000.00 (ten million rupiahs), with the provision that if the victim is not paid, then the victim is replaced with a prison sentence for 1 (one) month and it has been stated that the accused Muhammad Farhan Balatiif alias Riinggo Abdiilah has been legally valid and proven legally convinced that it was wrong to commit defamation . Decision Number 11 of 2008 concerning Information and Transactions, because all of its elements have been proven valid and convincing based on the facts revealed in court.

Defaming someone's reputation in this context is not sexual in nature in the sense that insulting someone 's reputation with slander or humiliation usually damages someone 's reputation . This sense of honor is objectified in such a way that it has to be observed through specific behaviors whether someone feels offended or not in general. It can also be said that children are not yet able to experience this kind of violation , so is the most insane person . Therefore , wanting to insult these two types of people cannot be considered a crime.

Meanwhile, Deinda Berbeida's criminal is a prison criminal who has the goal of losing independence, while Deinda's criminal has the goal of property from the perpetrator of the crime . Kareina, deinda is a rule with emphasis on the obligation to pay something in the form of money because it violates a rule that applies in society.

Activities in electronic electronic transactions are robust and worrying about the consequences of phishing in Indonesia. This is also supported by the fact that internet users in Indonesia are spread across various groups of people, so they want to know the reliability of internet intelligence , one of which is the birth of internet crime, because cyber crime , especially phishing is a crime committed. with deception that not all users are aware of before.

So , of course, the behavior of cybercrime that roams the virtual world in the form of phishing must be subject to sanctions in the form of criminal liability for his guilt. So in addition to that, it should be noted that it is the victims of phiishiing who are the most independent. If the victim of financial loss is a victim of material loss , then for the welfare of the victim of financial loss and the victim of indirect financial loss (husband/wife, child or relative) should not be affected by material loss such as economic loss .[8]

The fundamental state must repay the victims of phishing what they deserve . This is also included in the rights of citizens to assurance, protection and legal certainty that is fair and just. Phiisiing is a form of intellectual crime called ideological theift . The term phisiing is a variant of the word or the term “fi shing” and refers indirectly to the use of increasingly sophisticated baits (baiits) that aim to obtain a catch (catch) of financial information and passwords from the intended party. And also, phishing is a form of activity that has the character of threatening or trapping someone with the concept of enticing that person . That is , by deceiving someone so that person indirectly provides all the information needed by the investigator.

Where is now rampant occurrence of criminal acts through computer networks . That is , by tricking someone into indirectly providing all the information the investigator needs . Phishing is a virtual world crime that is currently rife through computer networks . With the balance of the times, crime is becoming more and more common throughout the world. Because of that, many of the threats that occur today also occur through computers .

## 5. Conclusion

The increasingly widespread intellectual balance requires regulations and balancing regulations, principles or guidelines to guarantee the implementation of human rights guarantees. This is becoming more and more painful because cybercrime is increasing . Therefore , from the discussion above, we can conclude that it is in this social media account that everyone feels they have the right to express whatever is on their mind and then upload it in written form . It is very detrimental, people's awareness will write or reveal something in an unwise manner , so it happens that problems arise as a result of what they upload , one of which is the problem of defaming someone's good name . In fact, this problem is a form of crime in cyberspace (cyber crime) , especially in the form of phishing , which is a form of activity that has the meaning of threatening or trapping someone with the concept of believing in said person . That is , by deceiving

[8] Sutan Remy Syahdeini, *Crime & Computer Crime* (Jakarta: Grafita Main Library, 2009).

someone so that person indirectly provides all the information needed by the investigator.

Where is now rampant occurrence of criminal acts through computer networks . In the social mediation, there were cases of defamation , utterances of dishonesty and spreading of hoaxes. Not to mention the spread of computer viruses, hacking, carding, gambling, child pornography and others that are included in cyber crime . These crimes in the virtual world are committed by an individual or several groups through social media or other intelligence by means of producing readings that are filled with insults, blasphemous or SARA in nature , which means that the intended party feels their good name has been dropped . The policies of the Indonesian government have nothing to do with the applicable law . Law Number 11 of 2008 concerning Information and Electronic Transactions (UU IiTEi) is the first legal framework (cybeirlaw) that regulates the cyber world because of content and its broad scope in discussing cyber regulations such as the expansion of electronic evidence tools . this, such as recognition of electronic documents and criminalization of actions committed in the world virtual.

## References

Barda Nawawii Ariieif. Leslative Policy in Crime Control at Prison ManagementFund. Seimarang: Diiponeigoro University , 1994.

Diikdiik M, Eiliisatriis Gultom. Cyber Law Aspects of Law and Information Technology . Bandung: PT. Reifika Adiitama, 2009.

Diimas, Asrullah, Muh Hasrul, and Hiijrah Adhyantii Miirzana. " Legal Protection of Advocates On the Iinteirpretasii Obstructiion Of Justiicei" 5 (2021).

Diion Valeiriian. Pe neApproach Analogies in Indonesian Criminal Law a. Yogyakarta: Meidiia Section , 2017. si

Hariiyono, Akbar Galiih, and Frans Siimangunsong. " LEGAL PROTECTION OF VICTIMS OF THE THEFT OF PERSONAL DATA (PHIiSHIING CYBEiRCRIiMEi) IN CRIIMINOLOGICAL PEIRSPECTIVES " (nd).

Malunseingei, Leitiiciia M., Corneiliis Dj. Massiiei, and Ronald Ei. Roriei. "Enforcement of the Law Against Behavior and Victims of Cybercrime Criimei Beirbein for Phiisiing Dii Indonesia" (2009).

R, Soeisiilo. Ki tab Criminal Law Law. Bogor. Politeiiiia, 1995.

Sahrul mauludii. Watch out for Hoaxes: Be Smart in Facing ncemaran Good NameS, peech Ke be an Dan nci Hoaxes. Jakarta: Eileix Meidiia Komputiindo, 2018.

Sudarsono. Law case. Jakarta: Riineika Ciipta, 2002.

Suharto, Budii, and Arnold Bagas Kurniiawan. " Criminal Acts of Cybeircriimei for Behavio Falsification of Data lOn Siteus Ei-Commeircei (Phiisiing)." JHP 17 (Jurnal Hasi http://Research)5, no. 2 (2020): 57–61. nejurnal.untag-sby.ac.iid/iindeix.php/jhp17.

Syahdeiiiinii, Sutan Reimy. Computer Crime & Crime J. akarta: Grafiita Main Library, 2009.

Wiibowo, Miia Haryatii, and Nur Fatiimah. " Phiisiing's Threat to Meidiia's Social Users in the World of Cybeir Criimei." Threat of Phing Against Social Media Users in the World of Cyber Crime1 (2017): 5.

Wiidodo. Funding In Cyber Cri m Pe mi ste me . Yogyakarta: Aswaja, 2009.

Y, Maryono, B. Patmii Iistiana. Information & Communication Technology .Jakarta: Quadra, 2008.