Efforts to Overcome Web-Based Phishing Crimes in the World of Cyber Crime

Ahmad Redi[1], Nopit Ernasari[2]
redi.ahmad2010@gmail.com[1], nopiternasari94@gmail.com[2]

Universitas Borobudur[1, 2]

Abstract. Phishing is a form of fraud used to obtain personal information, such as passwords, credit card numbers, and other financial information by impersonating a trusted entity or website. In the context of web-based phishing crimes, perpetrators create fake websites that often closely resemble the official website of the entity they are impersonating, such as a bank, e-commerce company, or social media platform. Phishing perpetrators then distribute links or send fake emails to victims, trying to lure them into entering their personal information. After gaining access to this sensitive information, perpetrators can exploit victims in a variety of ways, including identity theft, financial fraud, and further cyberattacks. Web-based phishing crimes are a growing threat, and as perpetrators become more adept at orchestrating attacks, efforts to address web-based phishing crimes are critical to protecting individuals and business entities from financial loss, identity theft, and privacy violations.

Keywords: Prevention; Phishing; Cybercrime

1 Introduction

At present, the rapid development of science and technology has become an everyday reality and is even a non-negotiable demand of society. The primary objective of innovative improvement is to change human existence for a superior, more straightforward, less expensive, quicker, and more secure future. The improvement of science and innovation, particularly data innovation (Data Innovation) like the web, is developing quickly. Almost all areas of life utilize information technology in carrying out their activities. Starting from the fields of economics, education, health, government, banking, religion, and also the defense and security system of a country.

The role of information and communication technology in the era of globalization has placed it in a very strategic position because it presents a world without borders, distance, space, and time, which has an impact on increasing productivity and efficiency. The influence of globalization with the use of information and communication technology has changed people's lifestyles, developed a

MIC 2023, October 28, Jakarta, Indonesia

DOI 10.4108/eai.28-10-2023.2341807

new order of life, and encouraged social, economic, cultural, defense, security, and law enforcement changes. [1]

One interesting thing is that the process of globalization began when the progress and development of communication and information technology occurred. Indeed, initially, our life was communication between living creatures, especially us as humans who cannot survive without communicating with each other, so with the progress and development of communication and information technology we must make the best use of it.

The advantages of data and correspondence innovation, aside from having a positive effect, are likewise perceived as giving chances to be utilized for the purpose of carrying out new violations (cybercrime), so security endeavors are required. One might say that data and correspondence innovation resembles a two sided deal, where aside from making a positive commitment to working on human government assistance, progress, and civilization, it is likewise a potential and powerful means for committing unlawful demonstrations.

With progresses in computerized data innovation, individuals have entered a progressive business world (advanced upheaval time) since it is felt to be simpler, less expensive, more commonsense, and more unique to discuss and get data. Be that as it may, behind this large number of advantages, once in a while specific gatherings misuse the utilization of data and correspondence innovation, especially the Internet. They deliberately enter the website of a certain agency or institution and then commit crimes therein, either stealing data or destroying data, not even a little stealing money via the internet, such as hacking ATM PINs. Crimes like this are called cybercrime. The problem of cybercrime today should receive careful attention from all parties regarding the development of future information technology because this crime is one of the extraordinary crimes (extraordinary crimes) and is even perceived as a serious crime and transnational crime.) which always threatens the lives of the citizens of the nation and the sovereign state.

New crimes at this time need to be paid attention to by everyone, especially the government, to be able to make preventive and/or repressive efforts against these new crimes, where these crimes are committed in cyberspace and another term is cybercrimes. Cybercrime is another structure or aspect of contemporary wrongdoing that has gotten far reaching consideration globally. Volodymyr Golubev calls it the new type of hostile to social way of behaving.[2]

Cybercrime is one of the dark sides of technological progress which has a very broad negative impact on all areas of modern life today. Such concerns were also expressed in the Cyber Crime paper presented by ITAC (Data Innovation Relationship of Canada) at the Global Data Industry Congress (IIIC) 2000 Thousand years Congress in Quebec on September 19, 2000, which expressed that cybercrime is a genuine and developing danger to monetary and social improvement all over the planet. Data innovation contacts each part of human existence thus can electronically empower wrongdoing. In connection with concerns about the threat/danger of cybercrime, because it is closely related to economic crimes and organized crime (especially for money laundering purposes), the UN Congress on the Prevention of Crime and the Treatment of Offenders (which is held every five years) has also discussed the issue This. This issue of cybercrime has been on the agenda twice, namely at the VIII/1990 Congress in Havana and at the X/2000 Congress in Win.

Acts against the law in cyberspace are a very worrying phenomenon, considering acts of carding, hacking, fraud, terrorism, etc, and the spread of destructive information has become part of the activities of criminals in cyberspace. Unlawful acts that occur in cyberspace must have

something to do with why someone commits cybercrime because it is important to know that the cybercrime committed will cause harm to other parties.

Two things cause cybercrime to emerge, namely technical and socio-economic (social). In technical terms, it cannot be denied that technological progress can break the development of society. The success of this technology eliminates national borders, making the world very narrow. The connection between networks that are connected to other networks makes it easier for criminals to carry out their actions. The uneven distribution of technology makes one stronger than the other. This weakness is exploited by irresponsible perpetrators to commit criminal acts. And in socio-economic terms, cybercrime is a product of your economy. The global issue that is then linked to this criminal act is network security. Network security is a global issue that is being introduced at the same time as the internet, as an economic commodity, many countries in dire need of network security devices. Cybercrime is a major scenario of world economic activity. [3]

Based on the background described above, the problem of this research can be formulated as follows: What is the form of punishment for perpetrators of web-based phishing crimes in the world of cybercrime?; and How are efforts to overcome web-based phishing crimes?

2 Methodology

The exploration utilized recorded as a hard copy is regulating juridical. The wellsprings of legitimate materials utilized in this exploration are essential lawful materials and auxiliary legitimate materials. The essential materials utilized are legitimate books. [4] The sorts of approaches utilized in this exploration are the legal guideline approach, case approach, and lawful idea examination approach. The data processing method used is an analytical method which is then outlined in descriptive analytical writing.

3 Result and Discussion

The increasingly rapid development of information technology over time has made technology and information central to society. In this case, it is also a basic need for people to increase their daily productivity with fast access to information, which makes advances in information and communication technology change people's lifestyles and trigger social, cultural, economic, defense, security, and law enforcement changes.

Phishing is a form of internet crime called identity theft. Phishing is sending fake emails to a person company or organization by stating that the sender is a legitimate business entity, which is deliberately created to obtain personal information from the victim. [5] Phishing activities show that crimes in the form of fraud, sending fake emails or websites that appear to be genuine are sent to other people to lure someone into providing information in the form of user ID, password, pin, bank account number, and credit card number to the phisher. by utilizing computer technology.

Users' minimal knowledge of the technological tools used is a factor that causes phishing, so technology users must be equipped with some knowledge about the operation of technology because as explained above, minimal user knowledge is one of the factors that cause cybercrime to occur. There is a theory that states that crime is a product of society itself, meaning that society itself produces crime. [6]

What needs to be noted is that apart from being known as hacking or hacking, cybercrime has other terms, namely cracking or cracker, which have similarities and differences between hacking and cracking. One of the crimes committed by cracking or crackers is phishing because this crime aims to benefit oneself and of course harm other parties if they become victims of cybercrime in the form of phishing.

One might say that data innovation is at present a two sided deal on the grounds that separated from adding to expanding government assistance, progress, and human development, innovation is likewise a successful method for committing unlawful demonstrations. [7] Cybercrime is a criminal activity that takes advantage of developments in computer technology, especially the Internet. Cybercrime is an illegal act based on the development of internet technology and the use of computer technology. Cybercrime is a new form or dimension of crime today that has received widespread attention in the international world, the dark side of technological progress in the era of society 5.0 which has a very broad negative impact on modern life today.

Legal regulations for cybercrime in the form of phishing were previously regulated in Article 378 of the Criminal Code concerning fraud, as it is known that phishing is generally an act of fraud. Fraud as formulated in Article 378 of the Criminal Code is:

> "Any individual who, expecting to unlawfully help himself or someone else, by utilizing a bogus name or misleading poise, by duplicity or a progression of falsehoods, instigates someone else to surrender something to him, or to give him an obligation or discount a receivable, is undermined with for misrepresentation with a greatest jail sentence of four years."

Several elements are contained in Article 378 of the Criminal Code, namely:

1. Whoever,
2. to help yourself or others,
3. Unlawfully,
4. By utilizing a misleading name or bogus respect, by double dealing, or by a progression of falsehoods,
5. Mobilize other people, and
6. To hand over something to him, or to give a debt or write off a receivable.

Based on the elements described in Article 378 of the Criminal Code, it can be concluded that whoever is the subject means the perpetrator who commits a criminal act of fraud. There is an intention to benefit oneself or another person, meaning that there is an intentional act carried out as an intention (oogmerk). Furthermore, the act was carried out unlawfully, which means that the perpetrator of the fraud has no right at all to enjoy the profits, namely the results of the fraud. [8]

The Data and Electronic Exchanges Regulation has been approved and executed, which was at first shaped by Regulation Number 11 of 2008 concerning Data and Electronic Exchanges and afterward Regulation Number 19 of 2016 concerning Revisions to Regulation Number 11 of 2008

concerning Data was established. Furthermore, Electronic Exchanges that have been active as of recently.

Indonesia itself has an extraordinary regulation with respect to electronic-based exchanges, specifically Regulation Number 19 of 2016 concerning Changes to Regulation Number 11 of 2008 concerning Electronic Data and Exchanges. However, the current regulatory dilemma is whether these regulations, both at national and international levels, can reach and follow the progress of changing patterns of cybercrime itself along with the rapid development of internet technology sophistication to date. The more sophisticated the development of information technology, the more sophisticated the forms and modes of perpetrators who commit crimes will be. [9]

A regulation regarding the crime of phishing certainly requires legal certainty to ensure law enforcement is carried out by the state against the perpetrators of the crime of phishing. The Principle of Legal Certainty (het rechtszekerheidsbeginsel), the principle of legal certainty is a consequence of the state being based on law. Therefore, every regulation that is formed must be clear. Legitimate conviction alludes to the unmistakable, super durable, and steady utilization of regulation where its execution can't be affected by abstract conditions. [10]

Based on the principle of lex specialis derogat legi generali, this means that special legal rules are considered valid even though they conflict with general legal rules. It can be concluded that what currently applies to regulate how the legal regulation of cybercrime in the form of phishing is currently regulated by Regulation Number 19 of 2016 concerning Alterations to Regulation Number 11 of 2008 concerning Data and Electronic Exchanges since this Regulation is extraordinary in nature. As of now, phishing acts are controlled in Article 35 related to Article 51 passage (1).

This phishing act not only creates a site that appears to be similar to a genuine, official site but also this phishing act carries out an act of lying to deceive or mislead another person, causing that person to experience loss because the person's confidential personal information is known to the cybercrime perpetrator in the form of phishing. Therefore, the act of phishing can be subject to Article 28 passage (1) related to Article 45A section (1) of Regulation Number 19 of 2016 concerning Changes to Regulation Number 11 of 2008 concerning Data and Electronic Exchanges since it has committed a demonstration of lying.

Based on the IDADX report, the total number of complaints about phishing attacks in Indonesia has increased significantly. It was recorded that IDADX received 26,675 reports of phishing attacks in the first quarter of 2023. If we look further at the first quarter of 2023, the most cases of phishing attacks occurred in February with a total of 150,050 complaints. Meanwhile, the number in January was only around 7,665 cases, and in March there were 3,960 cases. [1]

The phishing case that occurred was carried out by a man named Steven Haryanto, who is a hacker and journalist. The man from Bandung deliberately created a genuine but fake website for the Bank Central Asia (BCA) internet banking service. Steven Haryanto bought domains with names that were almost similar to the original BCA Internet Banking site, namely "www.klikbca.com". The domain names he purchased were the domain names wwwklik-bca.com,klikbca.com, clickbca.com, klikbca.com, andklikbac.com. The appearance and contents of these sites are almost similar to the original site. If a BCA customer incorrectly types the domain name of the original BCA site, then the customer can fall into the trap of a fake site created by Steven Haryanto, especially as the customer enters personal information such as username and password, credit card number, PIN, account number, date of birth, or name. biological mother so that Steven Haryanto knows the customer's personal information. [12]

Based on the case above, Steven Haryanto can be charged with Article 35 of Regulation Number 19 of 2016 concerning Corrections to Regulation Number 11 of 2008 concerning Electronic Data and Exchanges because Steven Haryanto fulfills the elements in Article 35 by creating a fake site as if using the original site.

If Steven Haryanto, after creating the phishing site, then sends an email containing a URL link that directs to his fake website. In the contents of the email, the potential victim is instructed to update his personal information, and the victim follows the instructions in the contents of the email to update his personal information on the phishing website he has created the victim's personal information is known to Steven Haryanto, then Steven Haryanto can be subject to Article 28 of Regulation Number 19 of 2016 concerning Alterations to Regulation Number 11 2008 concerning Data and Electronic Exchanges since it has satisfied the components in Article 28 section (1) since it deliberately and without right gets out bogus and deceiving word which brings about buyer misfortunes in Electronic Exchanges.

The punishment imposed for cybercrime in the form of phishing is subject to multiple articles, namely Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) or Article 35 in conjunction with Article 51 paragraph (1), and cannot be more than the maximum penalty plus one third, This system is called a softened cumulation system. This is called "Concursus Realis". Concursus Realis occurs when a person commits several acts, and each act stands alone as a criminal and the criminal acts committed do not need to be similar or even need to be related to one another.

The implementation of Law No. 19 of 2016 in conjunction with Law No. 11 of 2008 is the latest chapter for the government of the Republic of Indonesia in fighting crime based on communication and information technology. This provision opens the way for law enforcers to take action and prosecute perpetrators of cybercrime. The faster the technology is used, the more vulnerable it is to existing crimes and those committed by parties who are not responsible for fraud, theft, and contamination of good names via the internet.

Criminal law policy is not an independent policy. Criminal law policy is part of efforts to overcome crime to improve the welfare of society. Actions to regulate society using criminal law are closely related to various policies in a social policy process that refer to broader goals. Efforts to overcome crime are with the main aim of protecting society to achieve social welfare. Broadly speaking, it can be divided into two paths, namely penal and non-penal paths. This also includes overcoming criminal acts of fraud using phishing methods to protect the people who are victims. Talking about society is a necessity or obligation that is attached to discussions about law. Law and society are two sides of the same coin. So without discussing society first, talking about law is empty. [13]

Law enforcement against cybercrime requires tools because the characteristics of this crime are carried out with both tangible and intangible tools. Determining the time and place where cybercrime occurs is determined by when the tool works effectively, therefore telematics analysis is very necessary for uncovering this crime.

Efforts to overcome the crime of phishing are by carrying out the initial steps of the investigator examining witnesses and examining proof of transfer, and then the investigator requests data for proof of a bank statement from the suspect's account number to the bank owned by the suspect and after obtaining the account owner's data which is suspected of being a reservoir for the inflow of money. The next step is for investigators to confiscate evidence in the form of 1 (one) email, 1 (one) ATM, 1 (one) photo file containing account mutations, and 1 (one) cell phone.

There are several other efforts to overcome web-based phishing crimes in the world of cybercrime, namely:

1. Always update information regarding phishing and new techniques used by cybercriminals. [14]
2. Internet users must always be alert to fake emails and websites that can be used by cybercriminals to carry out phishing acts. Internet users should check the sender's email address and make sure that it is truly from a trusted party.
3. Internet users must always increase account security by using strong and different passwords for each account. Internet users can also use additional security features such as two-factor authentication to protect accounts from phishing attacks.
4. The government can increase public awareness about the crime of phishing and how to avoid it. It can be done by conducting public campaigns and educating the public about the crime of phishing.

Efforts to overcome web-based phishing crimes in the world of cybercrime require cooperation from all parties, including the government, internet users, and internet service providers. By increasing awareness and skills in dealing with phishing crimes, we can reduce the number of victims and losses caused by phishing crimes.

The community's lack of legal awareness has implications for their understanding and disobedience to the law. There are several reasons formulated by Dikdik M. Arief Mansur and Elisatris Gultom that until now the legal awareness of the Indonesian people is still very lacking, namely: the legal awareness of the Indonesian people in responding to cybercrime activities is still felt to be lacking. This is caused, among other things, by the public's lack of understanding and knowledge (lack of information) regarding the types of cybercrime crimes. This lack of information causes cybercrime prevention efforts to experience obstacles, in this case, obstacles related to law compliance and the community's monitoring (controlling) process for any activity suspected to be related to cybercrime.

4 Conclusion and Suggestion

4.1 Conclusion

Phishing is a type of cybercrime that often occurs and attacks all online-based industrial sectors, such as e-commerce, social networking services, and banking. Punishment for criminal acts of web-based phishing in cyberspace, in the form of criminal threats for the perpetrator (phisher) which is regulated in Article 378 of the Criminal Code in general criminal regulations, while in extraordinary criminal guidelines, in particular controlled in Regulation Number 19 of 2016 concerning Revisions to the Law Number 11 of 2008 concerning Data and Electronic Exchanges, which is likely to layered articles, specifically Article 28 section (1) related to Article 45A passage (1) or Article 35 related to Article 51 section (1) and cannot be more than the maximum penalty plus In one third, this system is called a softened cumulation system. This is called "Concursus Realis". Concursus Realis

occurs when a person commits several acts, and each act stands alone as a criminal act and the criminal acts committed do not need to be similar or even need to be related to one another. Overcoming criminal acts of fraud through phishing methods can use penal or non-penal policies.

Penal measures aim to ensure that the perpetrator is responsible for his actions and can provide a deterrent effect to the perpetrator so that he does not repeat his actions. The punishment of web-based phishing crimes in the world of cybercrime is an important step in maintaining security and trust in the digital ecosystem. The crime of web phishing is a serious threat that can cause financial loss, identity theft, and privacy violations.

4.2 Suggestions

To overcome web-based phishing crimes in the world of cybercrime, several efforts can be made, including mapping threats, improving human resource skills, creating strong policies, establishing international cooperation, and increasing public awareness. Apart from that, internet users can also take preventive measures such as always updating information related to phishing, and always being alert to fake emails and websites. Apart from that, the legal regulations for online fraud in the form of phishing require changes to the ITE Law by concretely formulating the concept of phishing. This aims to strive for reform of criminal law so that justice can be achieved by developing a criminal law design based on restorative justice that is a deterrent.

There is a need for regulations that encourage the application of criminal compensation. According to the Restorative Justice Theory, the perpetrator should return what the perpetrator has taken from the victim. Internet users also need to increase their awareness and knowledge about phishing crimes and how to avoid them.

Reference

[1] B. M. P. Jombang, "PT. BPR BANK JOMBANG PERSERODA," 2023. [Online]. Available: https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya/#:~:text=Serangan%20phishing%20capai%2026.675%20kasus%20pada%20kuartal%20I%202023&text=Hal%20tersebut%20mengalami%20kenaikan%20sebanyak%2020.569%20laporan%20p. [Accessed 20 September 2023].

[2] S. Siswanto, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, Jakarta: PT. Rineke Cipta, 2009, p. 39.

[3] B. Nawawi, Tinda Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Jakarta: PT. Raja Grafindo Persada, 2005, p. 1.

[4] S. Lasmadi, "Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik," Jurnal Ilmu Hukum, pp. 40-41, 2021.

[5] B. J. Nasution, Metode Penelitian Hukum, Bandung: Mandar Maju, 2008, p. 84.

[6] a. hamzah, Delik-Delik Tertentu (Speciale Delicten) Didalam KUHP Edisi Kedua, Jakarta: Sinar Grafika, 2015, p. 100.

[7] M. Alfian, "Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan," Jurnal Kosmik Hukum, vol. 17, no. 2, pp. 149-150, 21 April 2017.

[8] S. R. Syahdeini, Kejahatan & Tindak Pidana Komputer, Jakarta: Pustaka Utama Grafita, 2009, pp. 63-64.
[9] A. W. d. M. Labib, Kejahatan Mayantara (Cyber Crime), Bandung: PT. Refika Aditama, 2010, p. 39.
[10] S. Rahardjo, Hukum dan Perilaku: Hidup baik adalah dasar hukum yang baik, Jakarta: Buku Kompas, 2009, p. 9.
[11] B. Suhariyanto, Tindak Pidana Teknologi Informasi (Cyber Crime), Bandung: PT. Refika Aditama, 2005, p. 24.
[12] Maskun, Kejahatan Siber (Cyber Crime) Suatu Pengantar, Jakarta: Kencana Prenada Media Group, 2013, p. 44.
[13] A. Y. S. Mario Julyano, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum," Jurnal Crepido, vol. 1, no. 1, pp. 13-22, Juli 2019.
[14] S. Kurniawan, "Niagahoster Blog," 17 July 2020. [Online]. Available: https://www.niagahoster.co.id/blog/mengatasi-phishing/. [Accessed 20 September 2023].