Law Enforcement Problems Against Cyber Crime Performed Through Phishing Method

Yusep Ardian¹, Ujuh Juhana², Haidan Angga Kusumah³
¹Universitas Muhammadiyah Sukabumi, Indonesia
²Universitas Muhammadiyah Sukabumi, Indonesia
³Universitas Muhammadiyah Sukabumi, Indonesia

ABSTRACT

Background. Technology can be said to be a "double-edged sword" because it is developing very rapidly, many people use it to make life easier, but behind that the speed of technology is used as a tool to commit crimes and create new problems in the form of cyber crime, namely phishing.

Purpose. The purpose of this research is to find out how law enforcement against cybercrime cases committed through the phishing method. The method used applies a qualitative method that focuses on looking at social phenomena that occur in society.

Method. The method used applies a qualitative method that focuses on looking at social phenomena that occur in society.

Results. The results showed that the Justice System has a major influence in the process of upholding law and justice starting from the Police level, the Prosecutor's Office to the Court Decision, besides that the ability of law enforcers to eradicate cybercrime is still limited in several ways such as, facilities and facilities, lack of expertise of law enforcement officials in handling cyber crackers, lack of police access to the latest information technology, and lack of public awareness and knowledge which will result in many obstacles.

Conclusion. The point is that the legal framework in the field of technology must be able to keep up with the rapid advancement of technology, although there are already laws governing these crimes, they need to be updated to reflect the progress of increasingly modern times and the variety of cyber crimes that may occur in the future.

KEYWORDS

Cyber, Fraud, Law Enforcement

INTRODUCTION

Indonesia is a state of law whose power is regulated and exercised according to applicable laws in all fields of life to promote justice and provide equal protection for everyone (Di Vaio dkk., 2020). Therefore, humans take advantage of technological developments that are advancing very quickly to meet their daily needs in conducting relationships between one another (Coppola dkk., 2019). Technology is currently developing very rapidly, many people use it to make life easier and for useful purposes ranging from the scope of work, education to household needs, but there are still many people who misuse it for purposes that harm themselves and even
Law Enforcement Problems Against Cyber Crime Performed Through Phishing Method

This cybercrime has the same nature that both the perpetrator and the victim are invisible, this is what makes the crime has its own complexity. The perpetrators of this type of crime can be a group of people doing business illegally or certain individuals.

In the case of this kind of crime, the perpetrators are certain people with very qualified knowledge and abilities in computer science (Morel dkk., 2020). The perpetrators usually know how to program computers well, and they can even see how computers work, find loopholes in the system and then commit crimes (W.-Y. Yang dkk., 2019). Although there are laws in place today, including rules and penalties for cybercrime, it is still prevalent and very high in Indonesia, especially in the case of phishing crimes (Luque dkk., 2019). Not only that, this crime also often targets online banking users, where when users submit their names and passwords into a fake login form, cybercriminals can easily explore it, phishing is also usually done using sites such as the web, email, SMS, and social media platforms connected to the internet.

Website engineering methods can be used to commit phishing crimes that can lead to financial losses, identity theft, and account breaches. Indonesia Anti Phishing Data Exchange (IDADX) reported that in the first quarter of 2022, there were 3,180 reports of phishing crimes in Indonesia, in the second quarter there were 5,579 reports indicating that the number of phishers in Indonesia is currently increasing. The fact that the e-commerce industry is one of the second largest targets of phishing crimes, reaching 32% in the second quarter of 2022 after financial institutions, shows that the level of such crimes in Indonesia is relatively very high.

The ability of law enforcement in combating cyber criminals is still limited in several ways such as, constraints on tools (media), lack of expertise of law enforcement officers in dealing with cyber crackers, and lack of police access to the latest information technology (Reichstein dkk., 2019). Because so many individuals or countries are affected, crimes using phishing methods in Indonesia have recently become a significant legal concern, but its protection in Indonesia is still considered not optimal. This can be seen from the many cases of phishing abuse that lure victims into malicious sites, which causes a lack of security and strict monitoring on the part of users, and the law enforcement security system in Indonesia is still not running properly. Victims and perpetrators of cybercrime do not have to be in the same location at the same time, making it more difficult to identify the perpetrator and depending on the material value associated with the goal, the value of the loss caused is unlimited. Therefore, there is a need for proactive and reactive crime prevention in combating cyber crime.

As the author has done through field research at Sukabumi City Police that the level of cyber crime is still very high in 2023, even in web engineering crimes or known as phishing there was an increase this year compared to the previous year, many reports were received by the police but many cases did not even reach the realm of the Court due to lack of evidence and the difficulty of law enforcement officials in catching cyber criminals (Stuart dkk., 2019). The number of factors in eradicating a cybercrime starts from law enforcement, not even rarely reaching the court and being decided by the Judge (Nosyk dkk., 2021). The case that became the researcher's attention as well as the object of research was a case that had been decided in (Sukabumi District Court Decision Number: 148/Pid.Sus/2017/PN.SKB) Yudi Stira Alias Iwan together with his colleagues (each witness was prosecuted separately) succeeded in manipulating the creation of a website on behalf of BRI, namely www.info-pemenang-bri2015.blogspot.co.id where it displays images and writings related to BRI Bank which seems to have activities to distribute prizes and as if the lottery came others (Y. Yang dkk., 2019). With the growth of sophisticated crime in the form of cybercrime, the speed of technology is used as a tool to commit crimes and has created new problems (Paul dkk., 2021).
from BRI Bank and has harmed the party concerned. (Callhoff dkk., 2020). The increasing use of digital media in various aspects of modern life is a sign of the information age we are living in, because the internet is increasingly used, it offers many advantages for people to live their daily lives, but also makes it easier for certain people to commit a crime. The internet and technology, especially computer technology, are becoming more integrated into everyday life as time goes by. The internet and computers have many benefits, but they also have a bad side that threatens to end human existence itself, because information technology is becoming increasingly important and as the Covid-19 pandemic spreads the threat is increasing until now (Pretorius dkk., 2021). The existence of development technology is a "double-edged sword" because in addition to providing many uses, it can also be used to commit crimes such as phishing (Stockwell dkk., 2021).

With the formulation of the problem as follows:

1. How is the Criminal Sanctions Against the Crime of Money Laundering in Indonesia.

This research is a normative legal study that focuses on analyzing the legal norm system, including principles, norms, rules of legislation, court decisions, and doctrine (Mao dkk., 2019). The research is prescriptive legal research analysis based on literature study, by analyzing legal issues through an understanding of legislation, literature, and other reference sources (Scarabottolo dkk., 2022). This research uses an empirical juridical approach with secondary data. Secondary data is obtained from the results of studies of legal literature and literature studies.

RESEARCH METHODOLOGY
In writing this article, the author applies a qualitative method that focuses on looking at social phenomena that occur in society [10]. The place and location of the research conducted was at Sukabumi City Police (Mao dkk., 2019). The data and data sources used are primary data such as the Criminal Code, Laws, Court Decisions that have binding force, as well as secondary data consisting of research-related books, journals and scientific articles, websites as well as internet sources used to help the author conduct analysis as information material. Data collection techniques related to the problems and difficulties of this research were collected or taken by the author by means of; literature study (Library Research), observation (Field Research) and interviews (Interview). This research is processed and analyzed by the stage of data collection in accordance with material law derived from primary legal materials and secondary legal materials which are then evaluated to provide prescriptive (Scarabottolo dkk., 2022). Researchers continuously analyze the data obtained, reduce irrelevant data, display data and interpret data.

RESULT AND DISCUSSION
Law Enforcement Against Phishing Crime Cases in the Indonesian Criminal Justice System
Police Level
Investigation
KUHAP defines investigation as a series of investigative efforts to search for and identify an event suspected of being a criminal offense in order to assess whether or not an investigation can be carried out in accordance with the procedures regulated in this law, namely article 1 point 5. As in the case of phishing crimes handled by Sukabumi City Police, it began with one of the public information that said in one of the houses in the Perum Genting Puri area Jl. Pangkane Kel. Cibereum Hilir, Kec. Cibereum Kota Sukabumi there are suspicious activities that get frequent
gatherings of a group of people in the house until late at night, until finally the Tipidter Reskrim Unit of Sukabumi City Police conducted a series of investigative activities against residents and at least information about activities in the house to find that the residence was inhabited by several men and one of the women (household assistant). The witness and the team then checked the house and found that there were 6 men, namely the defendant Yudi Stira and his colleagues.

When checking one of the rooms there were several electronic devices such as laptops, modems and mobile phones in a very suspicious position. After conducting an initial check of the electronic devices which the defendant admitted belonged to him and looking at the history of website usage, namely www.blogger.com which is connected to an email to create a website on behalf of BRI, namely www.info-pemenang-bri2015.blogspot.co.id and then checking with the naked eye by comparing the official BRI Bank website, namely www.bri.co.id with the site that the defendant created, it turns out that there are many differences.

Investigation

Investigation is a series of investigative steps carried out in accordance with legal approaches and guidelines to uncover and collect evidence to understand the crime that has occurred and identify the perpetrator. Given this, the main responsibility of an investigator is very important, namely to find and also collect evidence in such a way as to obtain:

1. Make light and identify a crime that occurred.
2. Can identify the perpetrators of the crime.

In cybercrime, information and communication technology is usually involved, therefore all evidence and evidence is very important for proof, but there are some characteristics that are unique to this cybercrime. The term "Information and Communication Technology" covers any technological tool used to process and transmit information, in a fairly broad definition it includes all processes involved in the handling, management and transfer of information across media, usually the evidence used in the case of phishing crimes by Sukabumi City Police include: mobile phones, laptops, website addresses, bank statements and screenshots.

For the stages of investigation carried out in this phishing case, after obtaining sufficient evidence and initial information from the defendant, then summon people to be heard and examined as suspects and witnesses, besides that, in carrying out the investigation process in this case, expert witnesses were invited because of the many difficulties faced by police officers, because only an expert is able to explain in detail about certain fields that are included in a criminal case or not. Because at this stage, the police have the authority to start from arrest, search and seizure, to detention. According to Article 1 Figures 5 and 14 of the Criminal Procedure Code, the initial evidence as a result of the police investigation becomes the basis for a decision by the investigator so that a person can be designated as a suspect or someone suspected of committing a criminal offense.

Level of Prosecution

Prosecution as referred to in Article 1 Point 7 is the act of the public prosecutor in submitting a criminal case to the relevant district court in terms of the procedures specified in the laws and regulations with a request to be reviewed and determined by a judge before the court.

In the case of phishing crimes, the prosecution is charged with a single indictment and at this stage the public prosecutor submits criminal charges which are basically as follows:

1. Stating that the defendant Yudi Stira Als. Iwan Bin Yudaside legally and convincingly committed the crime of "committing an act intentionally and without rights or unlawfully manipulating, creating, changing, removing, destroying electronic information and/or electronic documents with the aim that the electronic information and/or electronic
documents are considered as authentic data” as regulated in Article 35 Jo. Article 51 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions.

2. Sentenced the defendant to 1 year and 10 months imprisonment minus the period of detention, with an order to remain in detention.

3. Determine the evidence in the form of:
   a. 11 sheets of printouts of website screenshot images;
   b. 5 sheets of printouts of SMS Caster screenshots;
   c. 1 unit of silver color Acer brand laptop;
   d. 1 unit of red Acer Aspire One brand laptop;
   e. 1 unit of black Acer brand laptop;
   f. 1 unit Laptop brand Acer Aspire Series black color;
   g. 1 unit of Asus brand laptop in white color;
   h. 1 unit Laptop brand Asus black color;
   i. Email: labadi.inapisa89@gmail.com;
   j. 2 units of 16 PORT USB SIPOLAR brand black color;
   k. 32 units of Huawei brand modem;
   l. 32 pieces of Telkomsel Sim Card;
   m. 1 unit of Nokia brand mobile phone black and blue imei: 354853081880142;
   n. 1 unit of motorcycle brand Honda Beat Nopol: F-2732-ZE blue color, along with STNK an. Yudi Stira and BPKB No: 1-09163041;
   o. Cash Rp. 2,000,000 (two million rupiah);
   p. 1 unit of mobile phone brand Nokia black color X2-02 model type RM-694 with imei number: 356318/05/497490/8;
   q. 1 unit of mobile phone brand Nokia 105 black color imei: 359755067346920;
   r. 1 unit of black and blue Nokia brand mobile phone model: RM-1134, Imei number: 359755066484763;
   s. 1 unit mobile phone brand Oppo Neo 7 white color Type A33W, Imei number 1: 863089031962698, Imei 2: 863089031962680;
   t. 1 unit of black color Nokia brand mobile phone 105, Imei: 359755064176585;
   u. 18 pieces of BRI Bank ATM cards;
   v. 13 pieces of BNI Bank ATM cards;
   w. 8 pieces of Mandiri Bank ATM cards;

4. Determined that the defendant be burdened to pay court costs in the amount of Rp. 5,000 (five thousand rupiah).

**Trial Level**

After the submission of the case file from the public prosecutor, the court is authorized to carry out the judicial system in the form of examining, trying and deciding cases. In this phishing crime case, from the beginning to the end of the trial, the defendant did not present any mitigating witnesses and admitted that the crime had been committed by him, including:

1. The defendant was arrested/secured on Tuesday, May 09, 2017 at approximately 00.30 WIB at his residence and admitted that in April 2016 he had created several fake websites on behalf of Bank BRI as if they were distributing prizes.

2. The defendant recruited his five colleagues from the beginning to commit phishing crimes, and immediately informed them of their respective duties and roles.
3. In addition to the evidence, a letter from the Digital Forensic Examination Report of the Ministry of Communication and Informatics of the Republic of Indonesia, Directorate General of Informatics Applications, was also submitted.

4. The proceeds obtained from the act were used for daily living expenses and bought a laptop and motorcycle.

5. Based on the analysis of the website, it can be concluded: the website contains a logo belonging to BRI Bank, contains logos of other agencies such as: Police, Ministry of Communication and Information, Ministry of Social Affairs, and DKI Government, the website is not owned by Bank BRI because the domain used is a free domain name (using blogspot.co.id service and the contact number listed is different from the original website.

The panel of judges will consider whether, based on the aforementioned legal facts, the defendant can be declared to have committed the criminal offense charged against him.

To declare that a person has committed a criminal offense, the actions of the person must fulfill all the elements of the criminal offense charged to him; Considering, the elements contained have been fulfilled according to the law, including:

1. The element of every person.

2. Intentionally and Without Rights or Against the Law, Manipulating, Creating, Altering, Deleting, Destroying Electronic Information and / or Electronic Documents, with the Purpose that the Electronic Information and / or Electronic Documents Considered as Authentic Data.

Before imposing a sentence, it is necessary to first consider the aggravating and mitigating circumstances for the defendant, namely:

1. Aggravating circumstances:
   a. The actions of the defendant disturbed the community.
   b. The actions that have been committed defame PT BRI (Persero) Tbk.

2. Mitigating circumstances:
   a. The defendant admitted his actions so as to facilitate the trial.
   b. Has never been convicted.
   c. The defendant regretted his actions

JUDGE

1. The judge hereby declares the defendant Yudi Stira Als. Iwan Bin Yudaside, has been legally and convincingly proven guilty of committing the crime.

2. Sentenced the defendant to 1 year and 7 months imprisonment.

3. Stipulate that the period of arrest and detention served by the defendant shall be deducted in full from the punishment imposed.

4. Stipulate that the defendant shall remain in detention.

5. Determine the evidence submitted by the public prosecutor.

6. Charges the defendant to pay court costs of Rp. 5000.

AUTHOR’S VIEW

Bringing a criminal case, especially cybercrime, to court is difficult because the crime is more complex. The trial process is the same as any court case, but in this situation presenting expert witnesses is very important because not all lay people are aware of the issues involved. The evidence is not only based on expert witness testimony, but letters are also important. In this case, Judges make decisions independently, which means that they are not subject to outside pressure or influence when making decisions and are based solely on the facts proven in court and based on the
Law Enforcement Problems Against Cyber Crime Performed Through Phishing Method

Obstacles and Efforts of Law Enforcement Officials in Countering Cybercrimes

Obstacles to Law Enforcement Against Cyber Crime

1. Related to evidence
   Cybercrimes are increasingly prevalent every day, making it difficult to prove them with the narrow range of evidence today. Before stepping into the proof stage, several factors must be considered, among others, the search for evidence or evidence that may exist (found), including tools used to commit criminal acts, evidence that is the result of crime, and items that have a direct relationship with crime. However, obtaining evidence is not that easy, as stated by Mr. Devi Ginanjar Hartono Unit 3 Tipidter Satreskrim Polres Sukabumi Kota as a resource person, the difficulties that are often faced related to obtaining evidence include:
   1. Evidence that has been removed by the perpetrator (device).
   2. Websites that have been deleted.
   3. Deleted conversations or chats.
   4. Technical devices that are removed.

Infrastructure
Insufficient resources and law enforcement infrastructure will result in cybercrime not being maximally enforced. Similarly, Sukabumi City Police are still weak in relation to supporting infrastructure used to eradicate cybercrime, at the Polres level the standard tools used only rely on laptops and mobile phones. This shows the importance of having sufficient tools and facilities, because law enforcement will not run efficiently without adequate tools or infrastructure.

The infrastructure in question also includes knowledgeable and competent human resources (HR), effective management, adequate equipment, sufficient finance, and so on. If the author compares this, it feels very left behind because this facility is also a very important factor to be able to support and eradicate an increasingly high cyber crime.

Cyber Criminals
The most common obstacle in an investigation is that the address listed on the suspect's identity is fictitious, because the perpetrator can easily make an ID card with a fake name and address, change positions especially if the perpetrator is outside the inter-island area, use a high-tech device, and hide his identity by removing the telephone number so that his location cannot be traced.

Society
In addition to other difficulties in conducting law enforcement against crimes that occur in cyberspace, the community is also one of the inhibiting factors of the rapid advancement of Information Technology and its wide reach, this is due to the low understanding and awareness of cyber security, where there are still many people who are easily lulled by promos or prizes on social media or websites, which results in eventually falling victim to crime.

This lack of awareness and knowledge will later result in efforts to overcome cyber crime experiencing many obstacles, and in this case the limitations are related to law enforcement procedures as well as community supervision (controlling) of every action suspected of being related to cyber crime.
Law Enforcement Efforts Against Cyber Crime

1. Cooperation with other agencies
   The expertise and understanding of law enforcement officers in dealing with cybercrime will certainly be affected by the lack of supporting infrastructure and resources. In this case, Sukabumi City Police does not have sophisticated tools, so the efforts made are to collaborate with POLDA because sophisticated tools and other supports are only available there.

2. Socialization
   To improve efforts in combating cyber crime, Sukabumi City Police has made efforts to educate the public about the dangers of the impact of crimes that occur in cyberspace and must be wise in using the internet. The socialization carried out so far is through public relations by going directly to the community, and through babin kamtinas with efforts to provide appeals through social media to the public about the dangers of cyber crime.

CONCLUSION

It can be concluded based on the research findings presented above that the existence and birth of phishing is part of the variety of crimes that occur in cyberspace as a result of the negative impact of the misuse of technology that is very rapid at this time, where the actions taken by the perpetrator trap or trick their victims who indirectly provide all the information needed. Based on law enforcement in the criminal justice system in Indonesia, phishing crime cases go through three stages of important components including the Police (investigation and investigation), the Prosecutor's Office (prosecution), and also the Court (examination until the judge's decision). In examining and bringing phishing crime cases to the Court realm is difficult because the crime is more complex and the trial process is the same as any Court case, but in this situation presenting expert witnesses is very important. The perpetrators of the crime can be subject to Article 35 of Law Number 19 of 2016 concerning Electronic Information and Transactions" being a legal basis for the crime of phishing. Therefore, in the phishing crime case handled by the Sukabumi City District Court, a verdict was obtained by sentencing the defendant Yudi Stira to 1 year and 7 months imprisonment.

Not only that, it can also be seen that law enforcement in Indonesia, especially Sukabumi City Police still has many certain weaknesses and has not fully implemented law enforcement optimally, especially in cybercrime cases, it can also be seen from various factors, including law, law enforcement, starting with finding and collecting evidence to catch cyber crime perpetrators is difficult to do, then there is the factor of facilities, which is still fixated and relying on laptops and cellphones while the crime continues to grow and results in lagging behind with various other cities which will result in the increasingly widespread cyber crime that occurs, the last is the community factor which still lacks awareness and understanding of the impact of cyber crime.

AUTHORS’ CONTRIBUTION
Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.
REFERENCES


