International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 10 October 2025

DOI: 10.47191/ijsshr/v8-i10-77, Impact factor- 8.007

Page No: 8200-8205

Law Enforcement of Phishing-Based Cybercrime in The Form of Application Package Kit (APK) Based on Electronic Information and Law

Rizky Rachmatika Wibisono[1], Ery Agus Priyono[2]

[1,2]Faculty of Law, Diponegoro University Jl. Imam Bardjo, South Semarang, Semarang City, Central Java

ABSTRACT: The rapid development of information and communication technology has changed the behavior of global society and has made the world borderless and caused social change. Cybercrime phishing involves fraudulently targeting individuals to provide personal information, such as login credentials or credit card numbers, by impersonating a trustworthy entity. This study aims to find out law enforcement against cybercrime with phishing methods linked to the Law. Information and Electronic Transactions. This research uses law enforcement theory. The results of the research on the factors that cause phishing-based cybercriminals to commit their crimes are due to financial motivation factors, the desire to make profits, the vulnerability of technological systems, and weaknesses in security infrastructure. Efforts to enforce the law on phishing-based cybercrime need to be maximized in preventing phishing-based cybercrime.

KEYWORDS: Law Enforcement, Cybercrime, Phishing

A. INTRODUCTION

The development of the current era is very rapid, Indonesia as a developing country is also affected by the changes of this era. Technology is one of them as a form of development of the times which has now become part of all living things on earth. So over time the rules have also changed because technology is also increasingly modern, allowing someone to abuse the system of technology itself.

The rapid development of information and communication technology is also related to the needs for daily human life. The internet one of the technologies born from the development of technology. Human life has also never escaped the internet. Overall, the Internet is a large interconnected network of computer networks that connects people and computers around the world, via telephone, satellite and other communication systems.

As a result of these developments, information technology itself has also changed the behavior of global society and human civilization. In addition, the development of information technology has made the world borderless and caused significant social changes that occur quickly. The use of internet media today is also quite a means that makes it easier for humans to get information and other things. All things become more practical in the internet world, but along with the practicality it brings, the internet also brings negative impacts in the form of security that cannot be guaranteed. Security in the cyber world is still very vulnerable due to the element of easy access to technology itself which causes many hackers who can easily reach a security system that is made in such a way, in the internet world there will always be gaps when talking about security systems, cybercrime was born.

In Indonesia, cybercrime is regulated in Law No. 19 of 2016 which is a revision of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions Various ways can be done to prove in court and investigations by the police in cybercrime, including optimizing the law, developing the knowledge and abilities of investigators in the cyber world, and adding and improving computer forensic facilities in the Indonesian National Police.

Cybercrime is an overall form of crime directed against computers, computer networks and their users, and traditional forms of crime using or with the help of computers. It can be concluded that cybercrime is any activity of a person, group of people, legal entity that uses a computer as a means of committing a crime, and a computer as a target of crime. Indonesia as a state of law, always prioritizes all state and community activities based on legal provisions.

Phishing is a form of cybercrime that involves tricking individuals into providing personal information, such as login credentials or credit card numbers, by posing as a trustworthy entity. The rise of digital technology has made phishing attacks more sophisticated and harder to detect, leading to an increased need for effective law enforcement strategies to combat this type of cybercrime. To effectively enforce the law against phishing, law enforcement agencies need to have specialized cybercrime units equipped with the latest technology and trained in the latest techniques. This includes the ability to conduct digital forensic investigations, trace digital footprints, and cooperate with service providers.

the internet to find and catch criminals.

One of the challenges in enforcing laws against phishing is that it is often difficult to identify the perpetrators. Phishing attacks can originate from anywhere in the world, making it difficult for law enforcement agencies to track down the perpetrators. Additionally, phishing attacks can be carried out anonymously, further complicating efforts to identify and prosecute the perpetrators.

Another challenge in enforcing laws against phishing is that penalties for this type of cybercrime can vary widely depending on the jurisdiction. In some countries, phishing is classified as a misdemeanor and carries only a small fine or a short prison sentence. In others, phishing is classified as a serious crime and carries much harsher penalties, such as long prison sentences and hefty fines.

In addition to law enforcement efforts, there is also a need to raise public awareness of phishing attacks. Many people fall victim to phishing attacks because they are unaware of the tactics used by cybercriminals. By educating the public about the risks of phishing and how to identify and avoid these attacks, we can reduce the number of victims and ultimately make it harder for cybercriminals to succeed.

One of the impacts of phishing-based cybercrime products that are currently busy is APK. Application Package Kit or abbreviated as APK is a file format used to distribute and install software and middleware to mobile phones with the Android operating system. Recorded until January 19, 2023, 483 Indonesians were affected by this APK-shaped phishing mode fraud. The police said that the total loss reached up to 12 billion rupiah. So here's how APK phishing-based cybercrime works:

1. The perpetrator will send a message in the form of an APK to potential victims with the mode that they are couriers from the expedition company.
2. Then the perpetrator asked the victim to open the message in the form of an APK.
3. After the victim opens the APK that has been sent by the perpetrator, a foreign application will be installed that will not be detected by the victim.
4. Once the foreign application is installed, this is where the victim starts the crime. The perpetrator can scavenge the victim's personal data information, so that if the victim has an m-banking application or "digital wallet", the perpetrator can access the application illegally and transfer the victim's money to the perpetrator.

The presence of Law No. 11/2008 on Electronic Information and Transactions in the use of Information Technology, media, and communication technology has changed the behavior of society and human civilization, especially in Indonesia. The development of information and communication technology has also caused the world to become borderless and caused significant social, economic, and cultural changes to take place so quickly. Information Technology is currently a double-edged sword because in addition to contributing to the improvement of welfare, progress and welfare improvement, it is also an effective means to commit acts. Currently, a new legal regime has emerged, known as cyber law or telematics law.

In detail, the contents of the article explain the acts that are considered unlawful according to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions in the form of website fraud. This law can be seen as the government's first step in dealing with cybercrime. Phishing crimes cannot be equated with ordinary fraud, because phishing actions utilize advances in technological systems.

The need for legal protection for internet users in the digital era is increasing Increasingly, there are still weaknesses in the current legal system. The Electronic Information and Transactions Law has not been able to cover all aspects of cybercrime and has not provided adequate protection for victims.

Countering phishing-based cybercrime is very important so that the public can be protected from the negative impact of these criminal acts. The government and the authorities must try to take effective measures to overcome this problem and provide protection for the community. , it is important to conduct a study and analysis on the countermeasures of cybercrime, so that effective solutions and efforts can be found to overcome this problem.

According to Article 9 paragraph (3), government PSEs are required to ensure that their electronic systems do not contain and do not facilitate the dissemination of prohibited electronic information or documents. Although the government, especially Kominfo, has regulated platforms that do not comply with the rules of the Electronic System Operator (PSE), there are still many cybercrime violations in the field. The use of increasingly sophisticated technology makes it easier for cybercriminals to carry out phishing activities. Therefore, the government needs to re-regulate the laws and regulations so that people can avoid phishing- based cybercrime.

This article will discuss what are the factors for the occurrence of phishing-based cybercrime and Law Enforcement related to phishing-based cybercrime based on the Electronic Information and Transaction Law.This research uses a normative juridical approach method. Normative juridical research is a problem approach by reviewing the laws and regulations. The normative juridical method is research to examine laws and regulations to solve problems. The normative legal method is a legal study conducted through the study of data or library materials, namely secondary data in the form of laws, theories, various literature, the internet, concepts, and scholars who explain the crime of gambling.

The specification used is descriptive-analytical. That is, providing a systematic and logical explanation in analyzing it. This is done

in order to review the applicable materials and literature, laws and regulations in Indonesia in relation to legal theories related to the problems systematically addressed by the . explained and analyzed. Factual, logical and reasoned.

B. DISCUSSION

1. Factors in the Occurrence of Phishing-Based Cybercrimes

In essence, technological development has a huge influence on people's attitudes. Technological and industrial progress is the result of human culture and besides having a positive impact, which is intended to be used for the benefit of mankind, it also has a negative impact on the development of human civilization itself.

Cybercrime or better known as cyber crime comes from the lives of those who exploit it and tend to increase their concentration in cyberspace from time to time. This development has an impact on the social life of the people and on the other hand, it also has an impact on the emergence of various forms of crime at the level of progress experienced.

One of the cyber crimes that is rampant today is phishing-based cyber crime. Phishing- based Cyber Crime has become an increasingly real and troubling threat in today's digital world. Phishing is a method used by criminals to obtain sensitive information such as passwords, credit card numbers, or personal data.

by posing as a trusted entity. In this endeavor, fraudsters use fake electronic messages, instant messages, or websites that appear genuine to fool unsuspecting victims. Within seconds, victims can be trapped and give their personal data to criminals without them realizing it. There are several factors that can lead to cybercrime. The following are some of the main factors:

1. Technological Advancements: Advances in technology and internet connectivity give cybercriminals more opportunities to conduct attacks. The presence of internet- connected devices and the widespread use of information technology gives attackers room to steal data, damage systems, or cause other disruptions.
2. Financial Gain: Cybercrime can result in substantial financial gains for the perpetrators. Cyber attacks such as identity theft, credit card data theft or ransomware can provide significant financial rewards for attackers. This financial drive is a strong motivation for them to engage in cybercrime.
3. Anonymity: One of the attractive factors of cybercrime is the ability to carry out attacks anonymously. Cybercriminals can conceal their identity by using tools such as virtual private networks (VPNs) or other techniques to hide their digital footprint. This makes it difficult for targeted parties or law enforcement agencies to identify and apprehend the perpetrators.
4. Lack of System Security: Many organizations or individuals do not have adequate security measures in place to protect their systems from cybercrime attacks. Weaknesses in security systems, software vulnerabilities, or lack of updates to vulnerable software can provide opportunities for attackers to enter and damage systems.
5. Human Factors: Often, cybercrime involves human factors. Perpetrators can take advantage of user ignorance or negligence to gain access to sensitive information. Phishing attacks, for example, involve sending fake emails that trick users into revealing personal information or logging into fake sites.
6. Political Conflict and Cyber Warfare: In some cases, countries or groups with specific political or military interests may conduct cyberattacks as a form of cyberwarfare. Such attacks may involve espionage, sabotage, or attempts to steal confidential information from other countries or organizations.

Criminological theory tries to understand some of the variables that can also affect laws, executive decisions, and law enforcement in the criminal justice system. The effectiveness of crime prevention strategies requires consideration of the factors that lead to crime. Social control theory can provide an understanding of the factors that influence the occurrence of criminal behavior in cyberspace. Some elements of social control theory can be linked to factors relevant to cybercrime, as follows:

1. Ties; Strong social ties with those around the individual can have an impact on cybercrime behavior. If individuals have strong bonds with their family, friends, or community members, they may be more likely to adhere to values and norms that prohibit cybercrime. In this case, social support and positive guidance from the environment can minimize the likelihood of individuals engaging in online criminal activities.
2. Engagement; Individual involvement in positive activities in the real world and the world of cyberspace can also influence the occurrence of . If individuals engage in activities that build positive skills and knowledge, such as education, work, or constructive hobbies, then they are less likely to engage in cybercrime.
3. Beliefs; Individuals' beliefs in their values and norms also play an important role in cybercrime. If individuals have a strong belief in the importance of respecting others' privacy, avoiding hacking, identity theft or spreading false information, then they are more likely to avoid cyber criminal behavior.
4. Skills; An individual's commitment to long-term goals and the investment they have in achieving those goals can influence cybercrime behavior. If individuals have skills and a commitment to positive technology development, such as cybersecurity, hacking ethics, and information security research, they may be more inclined to use their skills in legal and ethical ways.

2. Law Enforcement related to phishing-based cybercrime based on the Electronic Information and Transaction Law.

Phishing itself can be defined as an act of crime using social engineering techniques in carrying out its actions. The perpetrator of this crime has its own designation, namely phisher, which in phishing crimes the perpetrator seeks to deceive the victim with the main target of obtaining personal information or personal data from the victim such as username, password and credit card details. This can be one of the benchmarks in cyber law enforcement in Indonesia. Currently, Indonesia in handling cyber law refers to the provisions of Law No. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) which regulates several provisions relating to phishing activities or online fraud, Article 26 of the ITE Law which states that;

"Prohibits any person from accessing another person's electronic system without the right or against the law. In the context of phishing crimes, perpetrators who access without permission or by falsifying their identity to obtain the victim's personal data have violated this provision.". Then in article 30 of the ITE Law which reads;

"Prohibits any person from creating or disseminating false and misleading information that may cause harm or loss to others. In the context of phishing crimes, perpetrators who create or disseminate false and misleading information with the aim of obtaining the victim's personal data have violated this provision.".

Furthermore, regarding the prohibition of identity theft in Article 31 of the ITE Law, it is stated that "Prohibits every person from committing acts of identity theft or damaging the identity of another person by using a false identity or falsifying the identity of another person. In the context of phishing crimes, a perpetrator who uses a false identity or falsifies the identity of another person to obtain the victim's personal data has violated this provision". And continued with Article 45A of the ITE Law which emphasizes that: "Every person who intentionally and without right enters, sends, releases, broadcasts, or makes available Electronic Information or Documents that have insulting content and or defamation will be punished with criminal sanctions. In the context of phishing crimes, perpetrators who create fake websites or fake messages that deceive victims with the lure of fake prizes or promotions, can be punished with criminal sanctions. is seen as an act that damages one's reputation."

The context of phishing in the ITE Law falls into 3 main categories, namely manipulation, breach, and moving or transferring someone's data. In the manipulation category, perpetrators who send electronic mail (e-mail) that seems genuine can be charged with Article 35 jo. Article 51 of the ITE Law, as follows: "Every person who intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as authentic data shall be sentenced to a maximum imprisonment of 12 years and/or a maximum fine of Rp12 billion."

Furthermore, phishing activities can be categorized as an attempt to break into or break into a system If the perpetrator breaks into or breaks into a certain electronic system, using the victim's identity and password without right, he can be charged with Article 30 paragraph (1).

(3) jo. Article 46 paragraph (3) of the ITE Law, as follows: "Any person who intentionally and without rights or unlawfully accesses a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking into a security system shall be sentenced to imprisonment for a maximum of 8 years and/or a maximum fine of Rp800 million." The next phishing attempt is to move or transfer For the act of moving or transferring information and / or electronic documents belonging to the victim, for example the contents of an account, phishers can be charged with Article 32 paragraph (2) jo. Article 48 paragraph (2) of the ITE Law which reads: "Every person who intentionally and without rights or against the law by any means moves or transfers Electronic Information and / or Electronic Documents to the Electronic System of another person who is not entitled is sentenced to imprisonment for a maximum of 9 years and / or a maximum fine of IDR 3 billion."

In the case that the author discusses regarding phishing-based cybercrime in the form of Application Package Kit (APK), that what is done by the phishing perpetrator is included in the 3 main categories in the ITE Law. Where the process of phishing-based cybercrime in the form of Application Package Kit (APK) the perpetrator distributes an application in the form of a receipt file that has entered into fraud, and when the application has been installed on the victim's cellphone the application will later break into and transfer data from the victim. So that in the event of phishing a proof is needed in determining a criminal offense of the perpetrator.

In determining whether the perpetrator is guilty or not, evidence is needed in the criminal justice process. In criminal law, the principle of In criminalibus, probationes bedent esse luce clariores is known, meaning that in criminal cases, evidence must be brighter than . The explanation of evidence given or shown in court must be clear. More importantly, this principle emphasizes that evidence must be more than circumstantial. This principle shows that proof is the main thing that must exist, because without proof, a crime cannot be solved. For the proof itself, there must be at least two pieces of evidence. If there is only one, the person's actions cannot be tried. Evidence becomes a benchmark in determining the criminal justice process. The expansion of conventional evidence as contained in Article 184 paragraph

(1) of the Criminal Procedure Code introduces new evidence that is continuous and changes from time to time, but in its inclusion as evidence, Electronic Data or electronic evidence raises several problems, namely:

1. Problems regarding locus delicti (place of the crime), in cyber crime investigators find it difficult to determine the accurate location or place where the crime occurred. Because often the perpetrator can change or delete the "digital footprint" of device used to commit cyber crime or set different location from the actual location.
2. Problems regarding tempus delicti (the time of the criminal offense), investigators are not can determine exactly when a crime occurred, as cyber crcan often repeat the time and date of their actions.
3. The issue of proof is a problem for law enforcement officials. The evidence sought is related to everything that is used to support, commit and the results of cybercrime are very difficult to know because behind the sophistication of the internet network system there is also a gap for people who have the expertise to delete or destroy their identity and. sky. On the other hand, information technology is a technology with an open system that is impossible to push or close illegally, where anyone with skills in this field can control data, change data, there is to turn fake data into genuine fake data.

In this case, the law functions as a rechtzeken heid or giver of legal certainty, where if problems and problems occur there is legal certainty to be used as a guide by the whole community, making legal factors in the implementation of electronic transactions, especially in the banking sector, can be a guide for related parties, both law enforcers such as bank employees themselves and the community. As the meaning of legal certainty itself is an interpretation of written law that can be used as a guide to the community, as an effort to overcome an act that is considered against the law. Based on the description above, the things that the author can analyze in law enforcement related to phishing-based cybercrime based on the law on information and electronic transactions are as follows:

1. Enforcement Officials

In terms of law enforcement, the participation of law enforcement officials is needed. Things that are indeed a prerequisite in determining criminal offenses in cybercrime to determine a criminal process, in social life are accompanied by many crimes, so that punishment is required to pay attention to efforts to maintain and preserve the purpose of community life. Punishing criminals is of course something that must be done, in addition to deterring criminals, it is also part of the state's efforts to maintain domestic justice. Therefore, in the process of law enforcement, the quality and capability of each law enforcement officer is needed. Strengthening the function of law enforcement officers who are qualified both individually and organizationally and structured to unite communities of specialization in handling all types of cyber crime can provide a sense of trust in the community of course in the process of law enforcement in Indonesia.

2. Improved Facilities and Infrastructure

Every law enforcement officer, in an effort to enforce phishing-based cyber in the form of Application Package Kit (APK), contributes to upholding the law in Indonesia. Law enforcement officers cannot do their job properly if they are not equipped with commensurate facilities and infrastructure, which in this case is a set of good legal norms and principles. Therefore, the determination of facilities and infrastructure in supporting preventive actions in cyber law in Indonesia is very necessary. Law enforcement most likely cannot carry out its intended function without certain means or facilities to assist law enforcement officials. Therefore, it is fitting that in the process of law enforcement, a commensurate tool is needed in detecting phishing in the form of an Application Package Kit (APK) so that the enforcement of cyber law in Indonesia can be carried out optimally.

3. Special Law on Cyber Law in Indonesia

Initially, Law No. 19 of 2016 on the Amendment to the Law of Law Number 11/2008 on Electronic Information and Transactions (UU ITE) as a support for cybercrime. The framing that occurs in society is that the ITE Law is only a tool to silence activities on social media. Because if we relate it to cybercrime in the form of phishing in the form of Application Package Kit (APK), regarding the settlement of cases for phishing perpetrators with the provision of punishment in the form of imprisonment and / or fines. Victims of phishing who basically have a need to fulfill the material losses they experience, are contained in the Law on Witness and Victim Protection or called the UUPSK, which states that there is protection for victims and / or witnesses of criminal acts in the form of compensation, restitution and assistance. Therefore, the effectiveness of the ITE Law to this day is still questionable for law enforcement of phishing victims because it has not explicitly regulated the rights of victims.

C. CONCLUSION

The factors that cause phishing-based cybercriminals to commit their crimes are financial motivation, the desire for profit, vulnerability of technological systems, and weaknesses in security infrastructure. And the lack of public education on technology becomes a reference for perpetrators to commit phishing-based cybercrime.

Law enforcement efforts for phishing-based cybercrime need to be maximized in preventing phishing-based cybercrime. Because the ITE Law is considered ineffective in tackling phishing-based cybercrime, so the need for re-regulation. The importance of re- regulation is to regulate the misuse of technology. And there must be a special law regarding phishing-based cybercrime. A special law on phishing-based cybercrime will affect the quality of cyber law enforcement, so that it becomes optimal until finally it becomes an effective law in tackling phishing-based cybercrime.

The Indonesian government needs to pay attention to the problem of phishing-based cybercrime, because in this day and

age the issue still occurs frequently and there are still many perpetrators roaming out there who are not touched by law enforcement officials. The government also wants to pay attention to the impact phishing-based cybercrime because sometimes the amount of losses suffered by victims is very large.

Law enforcement officials need to improve cybersecurity because it protects against cyber attacks and cybercrime. As well as conducting socialization to educate ordinary people about the importance of phishing-based cyber crime in order to protect themselves from all forms of phishing-based cyber crime.

The Indonesian government and law enforcement officials need to take more decisive action in preventing phishing-based cybercrime. The Indonesian government needs to regulate specifically the regulation of phishing-based cybercrime. Then the need for special patrols in cyberspace by law enforcement officials to prevent phishing-based cybercrime.

REFERENCES

1) Ardi Saputra Gulo, Cyber Crime in the form of Phishing Based on the Electronic Information and Transaction Law, Journal of Criminal Law Vol. 1, No. 2, 2020, Page 4.
2) Dian Alan Setiawan, "Cyberterrorism And It's Prevention In Indonesia", Journal of Legal Media, Vol. 27, No. 2, 2020, pp. 268.
3) Hafsah, Web-based and Mobile Android Package (APK) Search Application with API, Vol 9, No 1, Informatics Engineering Study Program UPN "Veteran" Yogyakarta, 2012
4) Ibrahim Fikma Erdisy, Introduction to Cyber Law, 2019, Page 3.
5) Indarta, Yose, Fadhli Ranuharja, Cyber Security: Challenges in the Era of Industrial Revolution 4.0.Yayasan Kita Tulis, 2022, Page 23.
6) Mansur, Dikdik M. Arief. Cyber Law: Legal Aspects of Information Technology, Tiga Serangkai, 2005. Page 5.
7) Maulana, M. R., & Arif Firmansyah. (2023). Law Enforcement Against Business Actors who Mine in Forest Areas without Permits. Journal of Legal Science Research, 11-16.
8) Nurfitria, Indah. "Criminological Analysis of the Corruption Crime of Abuse of Authority in Government Positions in Bandar Lampung", Journal of Poenale, 3 (3), 2015 1-12 Page 6 Ronald E. Rorie, Law Enforcement Against Perpetrators and Victims of Cybercrime in theForm of Phishing in Indonesia, Vol. 11 No. 3, Lex Crimen, 2022, Page 4.
9) Umbara, A., & Setiawan, D. A. (2022). Criminological Analysis of the Increase in Cyber Crime during the Covid-19 Pandemic. Journal of Legal Science Research, 81-88.
10) Vikran Fasyadhiyaksa Putra Y, Modus Operandi of Phishing Crime according to ITE Law, Vol. 4 No. 6 Jurist-Diction, 2021