Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

Law Enforcement Against Cyber Crime in the Form of Phishing According to Law Number 1 of 2023 Concerning Criminal Code

Feberman Lahagu[1], Zetria Erma[2], Ramadhany Nasution[3]
Universitas Pembinaan Masyarakat Indonesia

Article Info
Keywords:
Phishing,
Cyber Crime,
Law Enforcement,
ITE Law.

ABSTRACT
The development of digital technology has given birth to various forms of cybercrime, one of which is phishing, which is a fraudulent act that utilizes social engineering techniques to steal victims' personal data. This study aims to examine the legal regulation of phishing crimes in Law Number 1 of 2023 concerning the Criminal Code, identify the factors that cause this crime, and evaluate the effectiveness of law enforcement in Indonesia. This research uses a normative juridical method with a legislative approach and document study. The results of the study show that the new Criminal Code has explicitly regulated the crime of phishing through Articles 332, 333, and 334 which include illegal access, destruction of electronic systems, and financial benefits from unauthorized access. However, because the law has not been fully enforced, law enforcement still refers to the ITE Law. The main factors causing the rise of phishing include low digital literacy of the community, limited law enforcement facilities, economic factors, and the sophistication of cybercrime modes. Therefore, there needs to be a synergy between adaptive regulations, increasing public awareness, and strengthening the capacity of law enforcement to face the challenges of cybercrime in the digital era.

Corresponding Author:
Feberman Lahagu
Universitas Pembinaan Masyarakat Indonesia
febermanlahagu2@gmail.com

INTRODUCTION

The transformation of information and communication technology has had a major impact on various aspects of the lives of the Indonesian people, while opening up opportunities and presenting new challenges, especially in the realm of cyber law. The increasingly widespread use of the internet and digital media makes cybersecurity issues such as digital attacks, the spread of hoaxes, and privacy violations increasingly important and urgent to be addressed, as they can affect the social and political stability of the country. Even though it occurs in cyberspace, cyber activities have real legal consequences, so traditional legal approaches are often inadequate to address these dynamics. If the typical characteristics of cyber activity are ignored, then many potential violations of the law will not be within reach of the existing legal system. Because these actions are based on electronic evidence, the perpetrator must be seen as having committed a concrete legal act. Therefore, the role of criminal law is not only as a regulatory tool, but also as a public policy instrument that must be in line with the direction of national development (Novita & Retnowati, 2024). This requires the birth of a holistic and

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

integrated legal policy, which relies on improving people's welfare and the effectiveness of law enforcement in dealing with the dynamics of crime in the digital era.

Phishing that is rampant is a form of crime as an act of disguising a website that aims to steal personal identities such as usernames, passwords and so on through the internet network or computer. The way phishing itself works is that the perpetrator of the phishing usually sends emails or messages from valid sources such as banks, wedding invitations and others, so that the victim gets the problem and fixes it by opening the website but actually the website has false information whose purpose is to steal the victim's personal data (Vadila & Pratama, 2021).

Indonesia, as one of the countries with an increasing number of internet users, is a vulnerable target for phishing crimes. Based on reports from various cyber security agencies, phishing cases in Indonesia are increasing every year, especially with the increasing number of digital transactions and electronic banking used by the public. Phishing attacks not only target individuals, but also companies, financial institutions, and government agencies, causing significant losses. Currently, criminal activities through computer networks are rampant. As time goes by, criminal activities are increasing around the world. There are so many threats coming through computers today. One of them is very prevalent in the social media environment which is a place where people can communicate remotely and get information quickly. Almost everyone in the world uses social media to socialize online so they don't have to meet in person (Febrika Ardy, Istiqomah, Ezer, & Neyman, 2024).

The phishing phenomenon in Indonesia shows an increasing trend from year to year. The BSSN report recorded thousands of phishing cases, mainly attacking banking, e-commerce, and social media platforms. This causes huge losses both economically and psychologically. Phishing does not only target individuals, but also government institutions and corporations (Sari, Rahmah, Zuhroh, Hidayat, & Rakhmawati, 2023). Along with the development of information technology, phishing crime modes have also evolved. If in the past phishing attacks were only carried out via email by sending fake links, now attack methods are increasingly sophisticated and varied. Some forms of phishing that often occur in Indonesia include: Email phishing, Website phishing, SMS and whatsApp phishing, Voice phishing (Vishing), Social media phishing and phishing pdf.

Crime arises due to various factors, such as economic pressure, social environment, opportunities to do wrong, and so on. In Indonesia, these factors have had a detrimental impact. Many individuals in society commit unlawful acts solely to provide for their livelihood. Today, in order to meet these needs, some people do not consider the consequences of their actions. This kind of attitude is clearly contrary to the moral values contained in Pancasila. In fact, not a few criminals are not afraid of law enforcement officials who are tasked with maintaining public order and security (Pratama, Mulyadi, & Arifin, 2017).

Cybercrime has become a worrying issue because it includes various illegal acts such as carding, hacking, fraud, digital terrorism, and the dissemination of harmful information. Criminal activities in the digital realm have a wide impact and significant losses, so they are the main highlight. Generally, acts of crime in cyberspace are carried out with a specific motive. It is important to realize that cybercrime can cause great losses to its victims. In

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

general, cybercrime includes various forms of crimes committed through the internet. Examples include theft of personal data, online-based fraud, malicious software attacks such as viruses and ransomware, distribution of illegal content such as child pornography, and hacking to obtain confidential information or important data. In addition, crimes such as cyberbullying, financial fraud, and attacks on the state's vital systems are also classified as cybercrimes (Fadli, Widijowati, & Andayani, 2024). These crimes have a serious impact on individuals, companies, and society as a whole.

Cyber security then became one of the problems in Indonesia that must be found a solution. The lack of public awareness about their personal data causes various types of cyber threats that will cause space to be created for a number of breaches and misuse of personal data. Cyber crime has several characteristics such as its actions do not result in physical violence (non-violence); lack of physical contact between the perpetrator and the victim (minimize of physical contact); Its actions depend on the use of technology and equipment such as telecommunication networks, media and informatics globally. The use of personal data requires good governance in the processing of data to be able to minimize cybercrimes that may occur. Therefore, strict and comprehensive regulations are needed to ensure full protection of personal data. Indonesia as a state of law (rechstaat) must be present to regulate all people's behavior based on the principle of equality before the law and provide guarantees of protection for this as outlined in the form of binding regulations as stipulated in article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia (Saly, Sulthanah, & Tarumanagara, 2023).

Therefore, public awareness and vigilance against the threat of phishing crimes is very important so that their personal information is not misused by irresponsible parties. The public needs to be more careful in recognizing indications of phishing, such as receiving emails or messages from unknown sources, the presence of suspicious links, or requests for unreasonable personal data. By increasing vigilance and implementing these preventive measures, people can protect their personal data from potential phishing attacks (Sutarli & Kurniawan, 2023)

As a form of crime that is rapidly evolving and continues to adapt to technological advancements, phishing requires a legal handling approach that is also adaptive and dynamic. Realizing this, Indonesia responded by making reforms to the criminal law through the ratification of Law Number 1 of 2023 concerning the Criminal Code (KUHP). This law is a new milestone that provides legal certainty against various forms of modern crime, including phishing.

This study aims to examine the legal regulation of phishing crimes in Law Number 1 of 2023 concerning the Criminal Code, identify the factors that cause phishing crimes, and evaluate the effectiveness of law enforcement in Indonesia. This research is expected to provide deeper insights related to the legal issues being studied, as well as be able to explore a broader understanding of the application and development of the law against cyber crimes, especially in the form of phishing according to Law No. 1 of 2023 of the Criminal Code. This approach is also expected to enrich theoretical understanding of criminal law in the digital era

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

METHOD

The type of research used in this writing is normative juridical, with a legislative approach. This research focuses on the study of positive law, namely the applicable written law, especially regarding the regulation of cyber crime in the form of phishing. The data sources used are primary data, namely relevant laws and regulations, including: Law Number 1 of 2023 concerning the Criminal Code, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), and secondary legal materials in the form of books, scientific journals, and relevant previous research results then collected through doctrinal studies and document studies. The data collection technique is carried out by reading, recording, and analyzing relevant legal materials through library research. The data analysis technique used is qualitative analysis, by categorizing and interpreting the data obtained, grouping information based on themes, and analyzing it to find relevant legal patterns or arguments.

RESULTS AND DISCUSSION

Regulation on Cyber Crime in the Form of Phishing in Indonesia According to Law Number 1 of 2023

In the realm of the new Criminal Code, cybercrime includes various unlawful activities carried out through the use of information and communication technology, such as computer devices, internet networks, and other electronic media. Based on Law Number 1 of 2023, forms of digital crime, also known as electronic crime or internet-based crime and in line with the definition of cyber crime internationally and in the Electronic Information and Transaction Law (ITE Law), are contained in the Chapter on "Crimes against Informatics and Electronics", especially in Part Five: (Hia, 2024).

1. Illegal access (Article 332);
2. Unauthorized use of electronic systems to damage or steal important information (Article 333);
3. Regarding financial gains illegally obtained from electronic systems (Article 334)

This law establishes severe sanctions for such violations to protect the security and integrity of electronic systems and information in Indonesia.

1. Article 332 of Law No. 1 of 2023 concerning Illegal Access
    a. Article 332 paragraph (1) of Law No. 1 of 2023 "Every Person who deliberately and without rights or unlawfully accesses the Computer and/or electronic system belonging to another person in any way, shall be punished with imprisonment for a maximum of 6 (six) years or a maximum fine of category V."
    b. Article 332 paragraph (2) of Law No.1 of 2023 "Every Person who deliberately and without rights or unlawfully accesses a Computer and/or electronic system in any way with the purpose of obtaining Electronic Information and/or electronic documents, shall be punished with imprisonment for a maximum of 7 (seven) years or a maximum fine of category V"
    c. Article 332 paragraph (3) of Law No.1 of 2023 "Every Person who deliberately and without rights or unlawfully accesses the Computer and/or Electronic System in any

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

way by violating, breaking through, exceeding, or breaking the security system, shall be punished with imprisonment for a maximum of 8 (eight) years or a maximum fine of category VI".

2. Article 333 concerning the unauthorized use of electronic systems to damage or steal important information.
   "Sentenced to a maximum of 7 (seven) years in prison or a maximum fine of category VI, Everyone who:
   a. Without the right to use or access the computer or electronic systems in any way, with the intent to obtain, alter, damage or eliminate national defense or international relations information that may cause interference or harm to the state or its relationship with the subject of international law;
   b. Without the right to take any action that causes the transmission of the program, information, code or command of the computer or state-protected electronic system to be damaged;
   c. Without the right or in excess of its authority to use or access the computer or electronic system, whether from within or outside the country to obtain information from the computer or electronic system protected by the state;
   d. Without the right to use or access any government-owned computer or electronic system;
   e. Without the right or in excess of its authority to use or access a computer or electronic system protected by the state, resulting in such computer or electronic system being damaged;
   f. Without the right or in excess of its authority to use or access a computer or electronic system protected by the community, resulting in such computer or electronic system being damaged;
   g. Affect or cause disruption of the computer or electronic system used by the government;
   h. Disseminate, trade, or otherwise exploit access codes or similar information, which may be used to break into computers or electronic systems for the purpose of misusing computers or electronic systems used or protected by government; or
   i. Commit acts in the context of international relations with the intention of damaging computers or other electronic systems that are protected by the state and are located in the jurisdiction of indonesia and are addressed to anyone."
3. Article 334 concerning financial gains illegally obtained from electronic systems.
   "Sentenced to imprisonment for a maximum of 10 (ten) years or a maximum fine of category VI, Any person who:
   a. Without the right or beyond its authority to use or access the Computer or electronic system with the intention of obtaining profits or obtaining financial information from central banks, banking institutions or financial institutions, credit card issuers, or payment cards€rn or containing the data of its customers' reports;
   b. Without the right to use data or access in any way the credit card or payment card belonging to another person in electronic transactions for profit;

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

c. Without the right or beyond its authority to use or access the Computer or electronic systems of a central bank, banking institution or protected financial institution, with intent to misuse, or to profit from; or
d. Spread, trade, or utilize Access Codes or similar information that may be used to break into Computers or electronic systems with the intent to misuse which may consequently affect the electronic systems of central banks, banking institutions or financial institutions, as well as domestic and foreign businesses.

Factors Causing Cyber Crime in the Form of Phishing in Indonesia

The development of various types of attacks in cyberspace is currently happening very fast and is becoming more widespread. This is exacerbated by the increasing number of smartphone users who are automatically connected to the internet, but not accompanied by an adequate level of digital literacy. Many users are not able to distinguish between correct or safe information, and are less aware of the potential for crime that can occur through cyberspace, especially through social media platforms that are now part of daily life. Technological advances have also changed the pattern of crime from those previously committed directly against physical objects, to long-range attacks over the internet. Perpetrators can access and collect victims' personal information in detail, one of which is through the phishing method, which is a fraud technique that disguises itself as a trusted party to steal the victim's data (Caniago & Sutabri, 2023).

There are several things that are factors that cause cyber crime in the form of phishing that occurs in Indonesia

a. Factors of Lack of Public Awareness
   The lack of awareness and knowledge of the community to face and protect themselves makes people vulnerable to becoming victims of cybercrime. Cyber crime is a despicable act and violates compliance in society and unlawful acts, although the Law specifically regulates cyber crime, it cannot be fully complied with and realized by all users of information technology services as a legal instrument. Until now, the legal awareness of the Indonesian people in responding to cyber crime activities is still felt to be lacking. This is due to the lack of public knowledge and understanding of the types of cyber crimes. where this can cause efforts to handle cyber crime to experience obstacles, in this case obstacles related to the legal structure and the process of community supervision of every activity suspected of being related to cyber crime.
b. Lack of Recommendations and Supporting Factors
   The lack of facilities and infrastructure in uncovering cyber crime cases is currently like sophisticated computer forensic equipment to prove cyber crimes. If the supporting facilities are not met, it is impossible for law enforcement to achieve its goals. The certainty and speed of case resolution depend on the supporting facilities in the fields of crime prevention and eradication. For this reason, special facilities or facilities for the purpose of investigating cyber crimes are absolutely necessary, especially by National Police investigators because they are at the investigation and/or investigation stage (Sriwulan, 2023).

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

c. Economic Factors
Economic factors are one of the main causes of cybercrime, especially in the form of phishing. Social disparities and high unemployment rates make some people look for shortcuts to earn money, one of which is through illegal activities in cyberspace. Phishing is an option because it does not require large capital, only electronic devices and internet networks. In an unstable economic situation, financially distressed individuals are more prone to commit these crimes.

d. User Negligence Factors
This is one of the main causes of cyber crime. Like people always enter all important data into the internet so that it makes it easier for some people to commit crimes.

e. The perpetrators are generally intelligent, have great curiosity, and are fanatical about computer technology.
The knowledge of computer criminals about how a computer works is far above that of computer operators. This is a difficult factor to avoid because many of the advantages or intelligence in accessing the internet that a person has in this day and age are misused for the sake of profit alone (Ketaren, 2017).

Law Enforcement Against Phishing Crimes in Indonesia

In general, law enforcement can be interpreted as the act of applying certain legal tools to impose legal sanctions to ensure the arrangement of the stipulated provisions, while according to Satjipto Raharjo, law enforcement is a process to realize the wishes of the law (namely the thoughts of the law-making body formulated in the legal regulations) into reality (Harefa, 2019).

As previously explained, cyber crime in the form of phishing is regulated in the latest Criminal Code, namely Law Number 1 of 2023 in Articles 332, 333, and 334. However, because the law has not been effectively implemented because the transition period has not reached three years since its ratification, currently law enforcement against cyber crime in the form of phishing is still regulated in law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). Cyber Crime in the form of phishing currently in Indonesia may be subject to Article 35 jo Article 51 paragraph (1) because phishing is a cybercrime that makes a site that resembles an official original site, even though the site is a fake site. Cyber crime in the form of phishing can also be subject to Article 28 paragraph (1) jo Article 45A paragraph (1) because phishing also commits lies to mislead others where directing the person who is lied to access a link where the link is directed to a fake website and gives an order to update his confidential personal information into a fake website that has been created by the phrying perpetrator, so that the confidential personal information is known to the phishing perpetrator and causes the person to suffer losses (Gulo, Lasmadi, & Nawawi, 2021).

Article 35 and Article 28 are based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which are formulated as follows:

1. Article 35 "Every Person intentionally, and without rights or against the law commits the manipulation, creation, alteration, omission, destruction of Electronic Information

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

and/or Electronic Documents with the aim of making such Electronic Information and/or Electronic Documents considered as if they were authentic data."
The criminal provisions are regulated in article 45A paragraph (1) "Any person who deliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions as referred to in Article 28 paragraph (1) shall be sentenced to a maximum of 6 (six) years in prison and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah)".

2. Article 28 "Every Person intentionally, and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions".
   The criminal provisions are regulated in article 51 paragraph (1):
   "Every person who meets the elements as referred to in Article 35 shall be sentenced to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah)".
   Although cyber crime in the form of phishing has been regulated in several regulations, there are still obstacles in handling cyber crime cases, as follows:
   a. Victims do not dare to report phishing crimes that occur because they are embarrassed and do not know the legal procedures. This happens because most victims feel ashamed of being deceived, especially when it comes to large amounts of material losses or touching personal domains such as sensitive data. In addition, many victims do not know the legal procedures that must be taken, both in making reports to the police, collecting evidence, and involving witnesses. The lack of understanding of legal mechanisms is a serious obstacle in law enforcement against phishing crimes. As a result, many cases are not officially recorded, making it difficult for the authorities to form a pattern of crime or arrest the perpetrators.
   b. Difficulties in law enforcement due to lack of evidence and limited resources of law enforcement officials both in professional abilities and in the ability to use technology. Phishing crimes often leave no physical traces, but rather digital evidence that requires specialized expertise to be legally identified, analyzed, and presented. Unfortunately, not all law enforcement officials have expertise in the field of digital forensics or cyber crime investigation. In addition, the limitations of tools and technological infrastructure in many regions also hampered the investigation process. Without technical competence and adequate tool support, law enforcement efforts against phishing crimes become less effective, and may even fail to uncover the perpetrators (Lokapala, Nurfauzi, & Widowaty, 2024).
   c. Changes in phishing crime modes along with technological developments and advancements. Phishing perpetrators always adapt their crime methods to advances in information technology. If previously they only relied on fake emails or fake websites, now perpetrators use fake applications, advanced social engineering techniques , and manipulation through social media. This rapid change in mode makes law enforcement officials always one step behind the perpetrators. Without regular updates to the understanding of modus operandi, the surveillance

Fox justi : Jurnal Ilmu Hukum
Volume 15, Number 03, 2025, DOI 10.58471/justi.v15i03
ESSN 2808-4314 (Online)
https://ejournal.seaninstitute.or.id/index.php/Justi

and legal protection system becomes irrelevant and vulnerable to cybersecurity system leaks.

d. Its nature is unlimited. This is because there are cases where the perpetrator committed a cyber crime of the phishing method originating from a correctional institution (prison). This should be unexpected because various kinds of technology are limited in prisons. Third
e. The location of the perpetrator was beyond the police's estimate. This is because perpetrators who have international networks commit cyber crim crimes of the phishing method abroad. It is not limited to any country. In fact, when tracking phone numbers, the perpetrator's location can change over time due to the technology they have (Dewantara, 2023).

CONCLUSION

Based on the results of the research, it can be concluded that *phishing crime* is a form of cybercrime that is growing rapidly along with the advancement of information technology. The ever-evolving modus operandi *of phishing*, from fake emails to dummy apps, makes it a serious threat to the security of personal data and public trust in the digital ecosystem. In a regulatory context, Law Number 1 of 2023 concerning the Criminal Code has explicitly regulated *phishing* crimes through Articles 332, 333, and 334, which include acts of illegal access, manipulation of electronic systems, and unlawful acquisition of financial gains. However, because this law is still in a transition period before it takes effect, law enforcement still refers to the ITE Law as the main basis for processing *phishing cases*. The main factors that cause the rise of *phishing* crimes in Indonesia include low public digital literacy, lack of legal awareness, weak law enforcement infrastructure such as digital forensic tools, as well as economic motives and user negligence in protecting personal data. On the other hand, technical challenges such as the lack of ability of law enforcement officials to deal with modern digital crime and the rapid change in the modus operandi of perpetrators make *handling phishing* cases often not optimal. Law enforcement against *phishing crimes* in Indonesia still faces various obstacles, including victims who are reluctant to report, difficulties in digital proof, and the location of perpetrators who are often outside national jurisdiction. Therefore, it is necessary to increase the capacity of law enforcement officials through digital technology training, adaptive legal policy updates, and synergy between institutions in preventing and eradicating *phishing* crimes. In addition, public awareness about the importance of maintaining personal data must also continue to be improved through massive and sustainable public education.

REFERENCE

Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayanan Di Universitas Bina Insan Lubuklinggau. *Jurnal Riset Sistem Informasi Dan Teknik Informasi*, *8*(1), 117–125.

Dewantara, G. M. (2023). *Penegakan Hukum Terhadap Pelaku Tindak Pidana Cyber Crime Metode Phising Oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta*.

Universitas Islam Indonesia Yogyakarta. Retrieved from https://dspace.uii.ac.id/handle/123456789/dspace.uii.ac.id/123456789/47616

Fadli, M., Widijowati, D., & Andayani, D. (2024). Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi. *Co-Value Jurnal Ekonomi Koperasi Dan Kewirausahaan*, *14*(12). https://doi.org/10.59188/covalue.v14i11.4335

Febrika Ardy, L. A., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2753

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Harefa, S. (2019). Penegakan Hukum Terhadap Tindak Pidana Di Indonesia Melaui Hukum Pidana Positif Dan Hukum Pidana Islam. *University of Bengkulu Journal*.

Hia, Y. (2024). Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber Dalam Kuhp Baru (UU 1/2023). *Jurnal Hukum Dan Bisnis (Selisik)*.

Ketaren, E. (2017). Cybercrime, Cyber Space, Dan Cyber Law. *Jurnal TIMES*, *5*(2), 35–42. https://doi.org/10.51351/jtm.5.2.2016556

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *5*(1), 22.

Novita, D., & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia : Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional, *4*, 1179–1186.

Pratama, F. A., Mulyadi, M., & Arifin, S. (2017). Kebijakan Hukum Pidana Terhadap Tindak Pidana Pencurian Dengan Modus Pecah Kaca Mobil Dalam Perspektif Kriminologi (Studi Kasus Putusan Pengadilan Negeri Stabat No. 404/Pid.B/2013/PN.Stabat), *5*(2), 124–133.

Saly, J. N., Sulthanah, L. T., & Tarumanagara, U. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewarganegaraan*, *7*(2), 1708–1713.

Sari, R. D. I. P., Rahmah, A., Zuhroh, F., Hidayat, T. R. P., & Rakhmawati, N. A. (2023). Analisis Bibliometrik Mengenai Serangan Phishing Pada Media Sosial Menggunakan Vosviewer. *Jurnal Ilmiah Informatika Komputer*, *28*(3), 230–240. https://doi.org/10.35760/ik.2023.v28i3.9514

Sriwulan. (2023). *tinjauan yuridis tindak pidana cyber crime di indonesia*. INSTITUT AGAMA ISLAM NEGERI PALOPO.

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *INNOVATIVE: Journal Of Social Science Research*, *3*(2), 42084221. Retrieved from https://j-innovative.org/index.php/Innovative

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2), 1–4.