Legal Study of Cyber Phishing Crimes Using Cyber Crime Legislation in Indonesia

Asep Wedotomo[1*], Sinarianda Kurnia Hartantien[2], Imam Suroso[3], Juli Nurani[4]
[1-4]Universitas Bhayangkara Surabaya, Indonesia

Corresponding Author's e-mail : *asepwedotomo@gmail.com*

ARMADA
JURNAL PENELITIAN MULTIDISIPLIN

e-ISSN: 2964-2981

ARMADA : Jurnal Penelitian Multidisiplin

https://ejournal.45mataram.ac.id/index.php/armada

Vol. 04, No. 06 Juni, 2026

Page: 1264-1269

DOI:

https://doi.org/10.55681/armada.v4i6.2093

Article History:

Received: Mei 03, 2026

Revised: Mei 12, 2026

Accepted: Juni 17, 2026

Abstract *:* The rapid development of information technology has led to the emergence of various forms of cyber crime, one of which is cyber phishing. However, Indonesian criminal law has not specifically regulated phishing as a distinct criminal offense, resulting in legal ambiguity and challenges in law enforcement. This study aims to analysis legal study of cyber phishing crimes using cyber crime legislation in Indonesia. This research employs a normative juridical method using a statutory and conceptual approach. The data used are secondary data consisting of primary, secondary, and tertiary legal materials collected through library research and analyzed qualitatively. The findings indicate that current regulations, particularly the Law on Information and Electronic Transactions (ITE Law), do not explicitly and comprehensively regulate cyber phishing, leading to uncertainty in its application. In addition, legal protection for victims remains limited, as the law primarily focuses on punishing offenders rather than providing effective compensation mechanisms. Furthermore, the new Criminal Code (Law No. 1 of 2023) has not accommodated phishing-related offenses involving personal data misuse. Therefore, legal reform is necessary to formulate clear provisions on cyber phishing and strengthen victim protection to ensure legal certainty and justice in the digital era.

Keywords : Criminal Law, Cybercrime, Phishing

Abstrak *: Perkembangan pesat teknologi informasi telah mendorong munculnya berbagai bentuk kejahatan siber, salah satunya phishing siber. Namun, hukum pidana Indonesia belum secara khusus mengatur phishing sebagai tindak pidana tersendiri, sehingga menimbulkan kekaburan hukum dan tantangan dalam penegakan hukum. Penelitian ini bertujuan untuk menganalisis kajian hukum terhadap kejahatan phishing siber menggunakan peraturan perundang-undangan kejahatan siber di Indonesia. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Data yang digunakan merupakan data sekunder yang terdiri atas bahan hukum primer, sekunder, dan tersier, yang dikumpulkan melalui studi kepustakaan dan dianalisis secara kualitatif. Temuan penelitian menunjukkan bahwa regulasi saat ini, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), belum mengatur phishing siber secara eksplisit dan komprehensif, sehingga menimbulkan ketidakpastian dalam penerapannya. Selain itu, perlindungan hukum bagi korban masih terbatas, karena hukum lebih berfokus pada pemidanaan*

pelaku daripada penyediaan mekanisme ganti rugi yang efektif. Selanjutnya, Kitab Undang-Undang Hukum Pidana baru (Undang-Undang Nomor 1 Tahun 2023) belum mengakomodasi tindak pidana terkait phishing yang melibatkan penyalahgunaan data pribadi. Oleh karena itu, pembaruan hukum diperlukan untuk merumuskan ketentuan yang jelas tentang phishing siber dan memperkuat perlindungan korban secara lebih optimal guna menjamin kepastian hukum dan keadilan di era digital.

Kata Kunci : *Hukum Pidana, Kejahatan Siber, Phishing*

INTRODUCTION

The rapid advancement of information and communication technology has significantly transformed various aspects of human life, particularly in the fields of communication, commerce, and financial transactions. However, alongside these developments, new forms of crime have emerged in cyber space, commonly referred to as cyber crime (Suseno, at al., 2025). One of the most prevalent and concerning forms of cyber crime is cyber phishing, a method used to deceive individuals into disclosing sensitive personal information such as passwords, banking credentials, and identity data (Budiyanto, 2025). The increasing number of phishing incidents in Indonesia highlights the urgency of establishing a clear and comprehensive legal framework to effectively address this issue and protect the public from digital threats (Firdaus, 2024).

Despite the growing prevalence of cyber phishing, the existing legal framework in Indonesia has not fully accommodated this form of crime (Azzahra, et al., 2025). Current regulations, such as the Law on Information and Electronic Transactions (ITE Law), primarily address general forms of electronic fraud and unauthorized access but do not explicitly define or regulate phishing as a distinct criminal offense (Hutabarat, 2023). This creates legal ambiguity and challenges in law enforcement, particularly in proving elements of the crime and ensuring consistent judicial interpretation. As a result, there is a significant gap between the rapid development of cyber crime techniques and the adaptability of criminal law in Indonesia (Munabari, Daryanto, Riyanta, & Hanita, 2024).

Several previous studies have examined cyber crime from various perspectives, including legal enforcement, cybersecurity measures, and digital fraud prevention (Karnasudiraja, 1993). These studies generally emphasize the importance of strengthening legal frameworks and technological safeguards to combat cyber threats (Tobing, 2024). However, most of these studies discuss cyber crime in a broad sense and do not specifically focus on phishing as a unique and evolving form of digital fraud (Tientcheu, 2021). Moreover, prior research often lacks a detailed analysis of the legal construction of phishing within Indonesian criminal law and its implications for victim protection (Asherli & Wiraguna, 2025).

The limitation of previous studies lies in their general approach to cyber crime, which does not sufficiently address the specific characteristics and legal complexities of cyber phishing (Sari, 2025). In addition, there is limited discussion regarding the inadequacy of current legal provisions and the need for future legal reform (ius constituendum). Therefore, this study seeks to fill this gap by providing a more focused and in-depth analysis of cyber phishing regulation within the Indonesian legal system, as well as evaluating the effectiveness of existing legal protection mechanisms for victims.

This research offers scientific merit and novelty by specifically examining cyber phishing as a distinct legal issue within the framework of Indonesian criminal law. It not only analyzes the current regulatory framework (*ius constitutum*) but also proposes future legal policy reforms (*ius constituendum*) to address existing shortcomings. Accordingly, the objectives of this study are to analyze the regulation of *cyber phishing* under Indonesian criminal law, to evaluate the legal protection available for victims, and to formulate recommendations for future legal development in order to ensure legal certainty, justice, and effective law enforcement in the digital era.

METHOD

This study employs a normative juridical research method, which focuses on the analysis of legal norms, principles, and regulations governing cybercrime, particularly cyber phishing, within the Indonesian legal system. The research adopts both a statutory approach and a conceptual approach. The statutory approach is used to examine relevant laws and regulations, such as the Law on Information and Electronic Transactions and the Indonesian Criminal Code, while the conceptual approach is utilized to analyze legal doctrines, theories, and scholarly opinions related to cybercrime and victim protection. The data used in this study are secondary data, which consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation and official legal documents related to cybercrime. Secondary legal materials consist of legal textbooks, scientific journal articles, and prior research findings that discuss cybercrime and phishing. Meanwhile, tertiary legal materials include legal dictionaries and other supporting references that assist in clarifying legal terminology and concepts. Data collection is conducted through library research, by systematically identifying, reviewing, and compiling relevant legal materials from various academic and legal sources. The collected data are then analyzed using a qualitative descriptive method, in which the author interprets and evaluates the legal provisions and theories to identify existing legal gaps and inconsistencies. Through this method, the study aims to provide a comprehensive understanding of the current legal framework, assess its effectiveness, and formulate recommendations for future legal policy regarding cyber phishing in Indonesia.

RESULT AND DISCUSSION

Regulation of Cyber Phishing under Indonesian Criminal Law

The findings of this study indicate that the regulation of cyber phishing under Indonesian criminal law remains fragmented, sectoral, and insufficiently specific. Cyber phishing is generally addressed through conventional fraud provisions, particularly Article 378 of the Criminal Code, and through several provisions in the Law on Information and Electronic Transactions (ITE Law). However, these legal instruments have not yet formulated phishing as an autonomous cyber offense with clear elements, scope, and legal consequences. This condition creates legal ambiguity because phishing does not only involve deception, but also digital manipulation, identity misuse, unlawful access to electronic systems, and unauthorized acquisition of personal data. In this context, the existing criminal law framework still tends to interpret phishing through conventional fraud doctrine, even though the modus operandi, evidentiary structure, and impact of phishing are more complex than ordinary fraud (Prasetio & Putra, 2025).

The problem becomes more significant when phishing is analyzed through the principle of legality in criminal law. A criminal act must be formulated clearly so that law enforcement officers, judges, victims, and society can understand the prohibited conduct. In phishing cases, perpetrators usually deceive victims through fake websites, fraudulent links, impersonation of institutions, false electronic messages, or social engineering techniques. These acts are difficult to place entirely within conventional fraud provisions because the core of the offense lies not only in inducing victims to suffer economic loss, but also in exploiting electronic systems and personal data. Therefore, the absence of a specific legal definition of cyber phishing may weaken legal certainty and create difficulties in proving the elements of the offense.

Furthermore, the lack of a clear legal construction of phishing leads to inconsistencies in law enforcement and judicial interpretation (Situmeang & Meilan, 2024). Law enforcement authorities often rely on a combination of provisions, such as fraud, illegal access, manipulation of electronic information, and personal data misuse. This combined approach may help fill regulatory gaps in practice, but it also creates interpretive uncertainty. Different investigators or judges may apply different articles to similar phishing cases, depending on whether they emphasize deception, data theft, unauthorized access, electronic document manipulation, or financial loss. Such inconsistency shows that the existing legal framework has not yet provided a stable normative basis for handling phishing as a distinct form of cybercrime.

The technological characteristics of phishing also show the limitation of existing legal instruments. Phishing attacks are dynamic, adaptive, and often transnational. Perpetrators can hide their identity, use anonymous digital infrastructure, operate across jurisdictions, and exploit

victims within a short period. Conventional criminal provisions were not designed to address this digital architecture. As a result, the legal process may face obstacles in identifying the perpetrator, tracing electronic evidence, proving intent, and connecting the phishing act with the resulting harm. This condition supports the view that cybercrime law must be able to respond to technological developments and not merely extend conventional criminal concepts into the digital space (Sutanto, Sulistyo, & Sugiarto, 2008).

In addition, the regulation of phishing cannot be separated from the issue of personal data protection. Phishing often targets sensitive personal data, such as usernames, passwords, banking credentials, identity numbers, credit card information, and other confidential data. Although Indonesia has enacted personal data protection regulations, phishing has not been fully constructed as an integrated offense that combines digital deception, illegal data acquisition, and potential economic loss. This gap shows that phishing should not be treated only as fraud, but also as a cyber offense that violates the victim's right to privacy, digital security, and control over personal data. The failure to recognize this multi-dimensional character may reduce the effectiveness of criminal law in preventing and prosecuting phishing cases.

The findings therefore demonstrate a gap between the rapid development of cybercrime techniques and the adaptability of Indonesian criminal law. The current regulatory framework still depends on scattered provisions, while phishing requires a more precise and comprehensive formulation. This finding confirms that Indonesian criminal law has not yet fully accommodated the specific nature of cyber phishing. Legal reform is needed not only to strengthen punishment, but also to clarify the elements of the offense, harmonize the relationship between the Criminal Code, the ITE Law, and personal data protection law, and ensure consistency in law enforcement. Without such reform, the handling of cyber phishing cases will continue to depend on broad interpretation, which may undermine legal certainty and the protection of victims.

Legal Protection for Victims and Future Legal Policy

The study also finds that legal protection for victims of cyber phishing in Indonesia remains limited and has not yet fully adopted a victim-oriented approach. Existing legal frameworks primarily emphasize the punishment of offenders, while the recovery of victims receives less attention. In phishing cases, victims may suffer financial loss, loss of access to digital accounts, identity misuse, psychological distress, reputational harm, and long-term vulnerability to further cybercrime. However, criminal law enforcement often focuses on identifying and punishing perpetrators rather than ensuring that victims receive compensation, restitution, data recovery, or practical assistance. This condition shows that the protection of phishing victims is still positioned as a secondary concern in the criminal justice process.

Although certain legal mechanisms allow victims to seek restitution or compensation, their implementation remains procedural, complex, and less accessible. Victims often face difficulties in proving the amount of loss, tracing the flow of funds, identifying the perpetrator, and navigating formal legal procedures. These difficulties become more serious when phishing involves anonymous accounts, foreign servers, digital payment channels, or rapidly deleted electronic evidence. As a result, the existence of legal protection does not always produce effective recovery for victims. This finding indicates that legal protection should not only be measured by the availability of legal norms, but also by the accessibility, speed, and effectiveness of remedies provided to victims.

The limited protection for victims also reflects the need to strengthen the restorative dimension of cybercrime law. Phishing is not merely a violation against public order or the authority of the state. It directly harms individuals whose personal data, economic interests, and digital identity are exploited. Therefore, criminal law policy should provide a balanced orientation between offender accountability and victim recovery. A victim-oriented framework should include mechanisms for restitution, compensation, account recovery, notification of data misuse, digital evidence assistance, and institutional support. Without these mechanisms, legal enforcement may result in punishment but fail to restore the victim's losses and sense of justice.

In terms of future legal policy or ius constituendum, this study finds a clear need to reformulate existing regulations by explicitly recognizing cyber phishing as a specific criminal offense (Oktarina, 2026). Such reform should formulate phishing as an act of deception through

electronic systems or digital communication that aims to obtain personal data, authentication credentials, financial access, or other unlawful benefits. The formulation should also include aggravating circumstances, such as phishing committed against vulnerable groups, phishing involving banking systems, phishing conducted by organized groups, phishing using institutional impersonation, and phishing causing large-scale personal data misuse. A clear formulation would help law enforcement officers determine the relevant legal basis and reduce inconsistency in applying criminal provisions.

Future regulation should also incorporate elements related to digital deception and personal data misuse more explicitly (Sutarman, 2007). The legal construction of phishing should not be limited to the consequence of financial loss, because many phishing cases begin with unauthorized data collection before any monetary loss occurs. Criminal law should recognize the unlawful acquisition, use, transfer, and exploitation of personal data through deceptive digital means as part of the offense. This approach would strengthen preventive protection because law enforcement could act before victims suffer greater economic loss. It would also align criminal law with the growing importance of personal data protection in the digital era.

Moreover, future legal policy should establish more effective victim protection mechanisms. These mechanisms should include accessible restitution procedures, cooperation between law enforcement agencies and digital platform providers, faster blocking of fraudulent accounts or websites, improved reporting channels, and stronger coordination with financial institutions. Victims should not bear the burden of recovery alone. The state, electronic system providers, and financial institutions should have clearer responsibilities in preventing harm, preserving evidence, and assisting victims. Such an approach would make legal protection more practical and responsive to the real nature of phishing victimization.

Strengthening the legal framework for cyber phishing would not only improve law enforcement, but also enhance legal certainty and justice for victims in the digital era (Widodo, 2011). Clearer regulation would provide guidance for investigators, prosecutors, and judges in identifying the elements of phishing and determining appropriate sanctions. It would also provide stronger protection for citizens who increasingly depend on digital services for banking, education, communication, commerce, and public administration. Therefore, the reform of cyber phishing regulation should be understood as part of a broader effort to modernize Indonesian criminal law in response to technological change.

Overall, the findings show that cyber phishing requires a more adaptive, comprehensive, and victim-oriented legal approach. The current legal framework still relies on fragmented provisions and has not fully addressed the specific characteristics of phishing as a digital crime involving deception, electronic systems, personal data, and financial harm. Legal reform should therefore focus on three main aspects: the explicit recognition of phishing as a distinct criminal offense, the integration of personal data protection into cybercrime regulation, and the strengthening of victim recovery mechanisms. These steps are essential to ensure that Indonesian criminal law can provide legal certainty, effective enforcement, and substantive justice in the digital era.

CONCLUSION AND SUGGESTIONS

This study concludes that the current regulation of cyber phishing under Indonesian criminal law has not yet provided a clear and comprehensive legal framework, as it still relies on general provisions that are not specifically designed to address the complexity of phishing practices. This condition affects not only the effectiveness of law enforcement but also the level of legal certainty for both authorities and society. In addition, the existing legal protection for victims remains limited, as the legal system primarily emphasizes punitive measures against offenders rather than ensuring adequate recovery and compensation for victims.

The findings of this research highlight the urgent need for legal reform that explicitly regulates cyber phishing as a distinct criminal offense, incorporates elements of digital deception and personal data misuse, and strengthens victim-oriented protection mechanisms. The implications of this study suggest that a more adaptive and comprehensive legal approach is essential to respond to the evolving nature of cybercrime in the digital era. Therefore, it is recommended that policymakers revise and harmonize relevant legal provisions, while law

enforcement institutions enhance their capacity in handling cyber-related offenses. These efforts are expected to contribute to greater legal certainty, improved victim protection, and more effective law enforcement in Indonesia.

ACKNOWLEDGMENT

The authors appreciate to Universitas Bhayangkara Surabaya dan for the support and facilitation during this research work.

REFERENCES

Asherli, B.F & Wiraguna, S.A,. (2025). Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022. Jurnal Hukum, Administrasi Publik Dan Negara, 2(4), 01–14. https://doi.org/10.62383/hukum.v2i4.290

Azzahra, M., Nurwati, Teguh Rama Prasja, & M Rendi Aridhayandi. (2025). Analisis Kasus Cyber Crime Di Indonesia Dan Tantangan Penegakan Hukum Dalam Menghadapinya. Jurnal Surya Kencana Satu : Dinamika Masalah Hukum Dan Keadilan, 16(1), 95–103. https://doi.org/10.32493/jdmhkdmhk.v16i1.47688

Budiyanto. (2025). *Pengantar cybercrime dalam sistem hukum pidana di Indonesia*. Banten: Sada Kurnia Pustaka.

Firdaus, R.A. (2024). Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4(1), 79-104. DOI: https://doi.org/10.14421/cf582q68

Hutabarat. (2023). *Cyber Law: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. Jakarta: PT Sonpedia Publishing.

Karnasudiraja, E.D. (1993). *Yurisprudensi Kejahatan Komputer*. Jakarta: CV Tanjung Agung.

Munabari, F., Daryanto, E., Riyanta, S., & Hanita, M. (2024). Cyber espionage in Indonesia: Legal challenges and the role of institutions in the digital era. Deviance: Jurnal Kriminologi, 8(2), 109–131. https://doi.org/10.36080/djk.3496

Oktarina. (2026). *Dinamika hukum dan perkembangan kejahatan di masyarakat*. Jakarta: Prenadamedia Group.

Pouani Tientcheu, P. (2021). Security awareness strategies used in the prevention of cybercrimes by cybercriminals (Doctoral dissertation, Walden University). Walden Dissertations and Doctoral Studies.

Prasetio & Putra. (2025). Cyber Crime: Penyalahgunaan Teknologi di Mata Hukum. Malang: Universitas Brawijaya Press.

Sari, R. M. P. (2025). Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia. Jurnal Hukum Dan Keadilan, 2(5), 49–55. https://doi.org/10.61942/jhk.v2i5.418

Situmeang & Meilan. (2024). Evolusi kejahatan dan pemidanaan: Tantangan dalam penegakan hukum dan penologi modern. Res Nullius Law Journal. 7(2). 87-97. https://doi.org/10.34010/rnlj.v7i2.15913

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Tiarma, B. A. N. (2025). Cybercrime in the New Criminal Code in Indonesia. Cogent Social Sciences, 11(1), Article 2439543. https://doi.org/10.1080/23311886.2024.2439543

Sutanto, Sulistyo, & Sugiarto. (2008). *Cybercrime Motif dan Penindakan*. Jakarta: Pensil 324.

Sutarman. (2007). C*yber Crime Modus Operandi dan Penanggulangannya.* Yogyakarta: Laksbang Pressindo.

Tobing, C. I., Surya, T. M., Roesa Selvias, L., Rehulina Girsang, S., Berliana Azzahra, P., Yolanda Purba, L., Agnia Putera, M., & Rusmana, N. (2024). Globalisasi digital dan cybercrime: Tantangan hukum dalam menghadapi kejahatan siber lintas batas. Jurnal Hukum Sasana, 10(2), 105–123. https://doi.org/10.31599/sasana.v10i2.3170

Widodo. (2011). *Aspek Hukum Kejahatan Mayantara*. Yogyakarta: Aswindo.