JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 2 Mei 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i2.10602/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Cyber Law Analysis and Customer Protection in Cases of *Phishing in* Digital Banking

Maria Minerva Gani[1], Cheryl Nathania[2], Putra Dirgantara[3], Heigel Ritonga[4], Rifaldo Aditya[5], Nicole Eugenia Yuri[6], Nathasya Jhonray Siregar[7], Tasya Amira Frananda Siregar[8]
[1]Prof. Dr. Yuni Priskila Ginting, S.H., M.H., Indonesia

Article Info

Article history:
Accepted: 30 April 2026
Publish: 9 May 2026

Keywords:
Phishing;
Social Engineering;
Criminal Liability;
Personal Data Protection.

Abstract

This study examines phishing in digital banking services as a form of cybercrime that combines electronic system manipulation and social engineering. Phishing is not merely a technical security issue, but also a legal problem involving criminal liability, consumer protection, and personal data protection. This research uses normative legal research with statutory and case approaches, particularly by analyzing phishing practices involving fake banking websites that resemble official digital banking platforms. The findings show that phishing can be legally constructed through several provisions under the Electronic Information and Transactions Law, the Personal Data Protection Law, and the National Criminal Code. The perpetrator's liability may be established through the elements of unlawful act, intent, capacity to be held responsible, and the absence of justifying or excusing grounds. In addition, victim protection must be carried out through preventive measures, responsive handling, and recovery mechanisms, including strengthening digital security, improving customer literacy, conducting internal investigations, and providing dispute resolution channels. Therefore, the prevention and handling of phishing in digital banking requires an integrated approach that combines criminal enforcement, banking governance, consumer protection, and personal data protection.

Corresponding Author:
Prof. Dr. Yuni Priskila Ginting
Dosen Hukum Universitas Pelita Harapan Karawaci, Indonesia
Email Correspondent: yuni.ginting@uph.edu

1. INTRODUCTION

The development of digital technology in the banking world has made it easier for people to conduct financial transactions quickly and efficiently. However, behind this progress, various types of cybercrime are emerging, one of which is phishing. Phishing is a type of fraud carried out by pretending to be an official entity to obtain sensitive user data, such as user IDs, passwords, PINs, and OTP codes, through fake platforms that resemble legitimate services. While this digitalization has significant benefits in supporting people's economic activities, it has also created opportunities for various types of cybercrime that are increasingly complex and difficult to detect.

One of the most common types of cybercrime is p*hishing*. *Phishing* is a fraudulent method that involves manipulating victims into providing sensitive information, such as user IDs, passwords, PINs, or OTP codes, through platforms that appear to be official. This method often exploits users' psychological weaknesses, such as panic, lack of digital

literacy, and trust in visual appearances that resemble official institutions. In the banking world, *phishing has* become a serious threat because it can directly cause financial losses for customers.

Case *phishing* the incident that befell a customer of PT Bank Central Asia Tbk (BCA) shows that this crime is still a relevant phenomenon in Indonesia. According to news reports, several customers suffered losses amounting to billions of rupiah after visiting fake websites impersonating the KlikBCA Bisnis service. Victims initially intended to access the official website but were instead redirected to a fake website with an address and appearance that closely resembled the legitimate site. When victims entered their banking details, the perpetrators misused the information to conduct transactions without the account holder's knowledge or consent.

This phenomenon shows a shift in crime patterns from those previously based on systems (*system-based crime*) to being user-manipulated (*user-based exploitation*). In many cases, *phishing*, the banking system did not experience a direct breach, but rather the perpetrator exploited user negligence or carelessness when accessing digital services. This is reinforced by BCA's statement confirming that the banking system remains secure, and that the incident was caused by customer access to a fake website. Thus, the weakness in this crime lies not only in the technological aspect, but also in the human factor (*human error*).

Human Error in the case of *phishing* is caused by customer negligence in verifying the authenticity of the sites they access, especially carelessness in checking domain addresses (*URL*), which is a key indicator of the legitimacy of digital services. Customers often rely solely on visual similarities without verifying security aspects such as site protocols or link sources, easily falling prey to fake websites that look like legitimate services.

Furthermore, errors also occur when customers knowingly enter sensitive data such as user IDs, passwords, and OTP codes into unverified platforms, which are then exploited by perpetrators to illegally access accounts. Another factor contributing to human error is psychological manipulation (*social engineering*) that causes victims to act hastily without conducting further checks, as well as a lack of compliance with the bank's security advisories. Thus, human error in this context is not only technical but also reflects users' low level of vigilance and digital literacy in dealing with cybercrime.

On the other hand, this case raises important legal questions about customer protection in the digital banking system. In the relationship between banks and customers, there is a principle of prudence (*prudential principle*) and the bank's obligation to maintain the security of its systems and customer data. However, when losses occur due to third-party phishing, debate arises about the extent of the bank's responsibility for those losses. Is the bank still liable for customer losses, or is the customer considered negligent for not being careful in protecting their personal data?

Furthermore, from a consumer protection and cyber law perspective, this case also relates to several existing regulations, such as the Electronic Information and Transactions Law (UU ITE) and personal data protection policies. These regulations are primarily intended to provide legal certainty and protection for digital service users, but in practice, their implementation often faces various challenges, particularly in addressing cross-system crimes and proving fault.

Based on the explanation above, it can be seen that *phishing* in digital banking services is not just a technical issue, but also involves legal aspects, the responsibilities of related parties, and customer protection as consumers.[1]Therefore, through research on *phishing* in digital banking services, especially in the mode of using fake sites and *social engineering*

that resembles official banking services, the author wants to analyze legal issues that are not only related to the technical aspects of system security, but also concern the criminal liability of the perpetrator, regulatory integration, data protection, and the legal interests of customers as victims.

Thus, this research is directed to answer two main problems, namely, how the law regulates criminal acts. *Phishing* and *social engineering in* digital banking services based on the Electronic Information and Transactions Law, the Personal Data Protection Law, the National Criminal Code, and regulations in the financial services sector, as well as how the perpetrators are held criminally responsible and efforts to protect the victims' data in criminal acts, *phishing* in digital banking services, both through preventive, responsive, and customer loss recovery efforts[2].

2. METHOD

This research is a normative legal study that focuses on applicable legal regulations. It examines how these regulations are applied in real-life situations. This method was chosen because the research aims to understand legal protection for customers in digital banking services. Furthermore, this study also discusses the bank's responsibility in the event of a *phishing crime*. Thus, this method is considered suitable for answering the research problem.

The approach used in this research includes a legislative approach (*statute approach)* and a case approach (*case approach*). The legislative approach is carried out by studying various relevant legal provisions, such as Law Number 11 of 2008 concerning Information and Electronic Transactions as amended, Law Number 8 of 1999 concerning Consumer Protection, and the Financial Services Authority (OJK) regulations relating to consumer protection in the financial services sector. This approach aims to understand the legal framework governing the relationship between banks and customers in the use of digital services.

Next, a case-by-case approach was employed by analyzing a phishing case involving a PT Bank Central Asia Tbk (BCA) customer, as reported in the media. The case analysis was conducted by examining the chronology of events, the perpetrator's modus operandi, and the bank's response. This approach was used to connect applicable legal norms with actual practices, thus identifying emerging legal issues and offering possible solutions.

The type of data used in this study is secondary data, consisting of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations related to the research topic. Secondary legal materials consist of scientific journals and articles from trusted media outlets, such as Kompas and AntaraNews, that discuss the crime of *phishing* in the digital banking sector. Meanwhile, tertiary legal materials include legal dictionaries and other sources that support the understanding of research concepts.

Data collection techniques were carried out through literature studies (*library research*), namely by collecting, inventorying, and analyzing various relevant legal materials. These legal materials were then classified by type and level of importance to facilitate the analysis process. Next, data analysis was conducted qualitatively using a descriptive-analytical method, namely by describing existing facts and then analyzing them based on applicable law. In this process, legal interpretation methods such as grammatical, systematic, and teleological interpretation were also used to gain a more comprehensive understanding. In this way, the research results are expected to provide clear and systematic conclusions.

The research process begins by identifying problems related to *phishing* in digital banking services. Afterward, the researcher formulated the problem to be discussed to focus the research. The next stage was collecting and processing legal materials through a literature review. The legal materials were then analyzed using a statutory and case study approach. In the final stage, the researcher drew conclusions to address the identified problems.

3. RESULTS AND DISCUSSION

3.1 Analysis of Elements of Criminal Responsibility

Case *phishing:* The crime targeting KlikBCA Bisnis customers constitutes a form of organized cybercrime that can be analyzed using a criminal liability framework. Legally, a person can be held criminally responsible if four cumulative elements are met: the existence of a criminal act, the capacity to be responsible, fault, and the absence of excuses or justifications. The normative basis for this case rests on Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions and its amendments (UU ITE) and Law of the Republic of Indonesia Number 1 of 2023 concerning the Criminal Code (KUHP), which has been in effect since January 2, 2026. The criminal liability framework in Article 36 of the National Criminal Code explicitly affirms the principle of no punishment without fault (*no punishment without guilt). This* case as a whole fulfills each of these elements, so that the perpetrator can be held fully accountable before the law. The following analysis systematically describes the fulfillment of each element of criminal responsibility based on the facts revealed in the case.

According to Article 35 of the ITE Law, it states that:

"*Any person who intentionally and without rights or against the law manipulates, creates, changes, removes, or destroys Electronic Information and/or Electronic Documents to make the Electronic Information and/or Electronic Documents appear to be authentic data.*"

From this formulation, three main elements must be fulfilled, namely the existence of an act of manipulation or active creation, carried out intentionally and without rights or against the law, and the aim is for the electronic information or document to be considered *authentic* by other parties. Article 28, paragraph (1) of the ITE Law, as amended by Law No. 1 of 2024, states that:

"*Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notices or misleading information that results in material losses for consumers in Electronic Transactions*"

The threat of a maximum prison sentence of six years and/or a maximum fine of IDR 1 billion, so that the elements include: the existence of a legal subject (any person), intentional distribution or transmission, content in the form of false or misleading information, and consequences in the form of material losses to consumers in electronic transactions. This is reinforced in Article 36 of the ITE Law as amended by Law No. 1 of 2024, adding a layer of aggravation by stating that:

"*Any person who intentionally and without right carries out an act as referred to in Article 30 to Article 34, which results in material loss to another person*," so that this article functions as an additional criminal act which increases the threat of criminal penalties if the actions in the previous articles have caused real losses which can be calculated economically.

The National Criminal Code (Law No. 1 of 2023) also complements this normative framework with more specific provisions for cybercrime in the banking sector. Article 332 of the National Criminal Code states:

"*(1) Any person who intentionally and without authority or unlawfully accesses another person's computer and/or electronic system in any way shall be punished by imprisonment for a maximum of 6 (six) years or a fine of up to category V.*
(2) Any person who intentionally and without authority or against the law accesses a computer and/or electronic system in any way to obtain electronic information and/or electronic documents shall be punished with a maximum prison sentence of 7 (seven) years or a maximum fine of category V.
(3) Any person who intentionally and without authority or against the law accesses a Computer and/or Electronic System in any way by violating, breaking through, exceeding or breaking through the security system, shall be punished with a maximum prison sentence of 8 (eight) years or a maximum fine of category VI.."[3]

Article 334 of the National Criminal Code specifically regulates crimes against the digital banking system with a maximum prison sentence of ten years, which prohibits, among other things:

a) accessing the electronic systems of banking institutions without the right to obtain benefits or customer financial information;
b) using data or accessing other people's credit cards or payment cards in electronic transactions to gain profit;
c) accessing the electronic systems of a central bank or protected financial institution with the intent to misuse or gain an advantage;
d) and distribute or utilize access codes that can be used to break into electronic banking systems.

The elements of a criminal act in this case are clearly fulfilled through a series of interrelated and inseparable actions. The perpetrator actively created a fake website that looked almost identical to the official KlikBCA Bisnis website owned by PT Bank Central Asia Tbk, not just by copying it visually but by designing a system that was able to record the victim's sensitive banking data in the form of PIN, OTP, and Appli Token Key in real-time. The act of creating this fake website directly falls under the formulation of Article 35 of the ITE Law, which prohibits the manipulation and creation of electronic information to be considered as authentic data, as well as Article 332 paragraph (3) of the National Criminal Code, which prohibits access to electronic systems by breaking through or overcoming security systems. The funds that should have been transferred to the victim's destination account were instead transferred to the perpetrator's account because the perpetrator had previously accessed the victim's KlikBCA account using data successfully obtained through the fake website, an act which is explicitly prohibited in Article 334 of the National Criminal Code which threatens a prison sentence of up to ten years for perpetrators who unauthorizedly access the electronic systems of banking institutions to gain profits. The entire series of actions was carried out without authorization, contrary to legal norms, and resulted in real material losses for the customer, thus Article 36 of the ITE Law, as amended by Law No. 1 of 2024, is also fulfilled as an aggravating provision. Therefore, the elements of a criminal act in this case are not only fulfilled formally and normatively, but also materially, because the resulting loss of customer funds amounting to billions of rupiah is a loss that can be concretely proven.

The perpetrator's fault in this case is not merely present, but also falls into the most serious form of fault in criminal law, namely full intent or dolus directus. All stages of the crime, from creating a fake website, optimizing search engines to get the site to the top, to utilizing digital advertising targeting potential BCA customers, demonstrate that the perpetrator not only intended his actions but also actively planned and controlled every consequence that arose from those actions. This construction aligns with the theory of will (*Wils's theory*), which states that intent is present when the perpetrator desires an act and desires its consequences, and in this case, the desired consequence is the transfer of funds from the victim's account to the perpetrator's hands. This evil intent has existed since the beginning of the planning, long before any of the victims accessed the fake site, which makes the element*s rema*in in this case, it is undeniable. This condition fulfills the requirements of intent as stated in Article 36 paragraph (2) of the National Criminal Code that acts that can be punished are crimes committed intentionally, and every element of intent must be proven at every stage of the case examination.

The perpetrator's capacity for accountability is strengthened, not weakened, by the level of technical sophistication employed in his modus operandi. Someone capable of building a fake website that is visually nearly indistinguishable from the official BCA website, managing SEO optimization, and simultaneously designing a clandestine banking data collection system is clearly an individual with a high level of technical mastery and full awareness of his actions. As Article 36 of the National Criminal Code emphasizes, criminal responsibility can only be imposed on someone who intentionally commits a crime, and the sophistication of the modus operandi in this case is evidence that the perpetrator was fully aware of the legal consequences of his actions. There is no indication whatsoever that points to a mental or intellectual disability as referred to in Articles 38 and 39 of the National Criminal Code that could be a basis for reducing or eliminating his capacity for accountability. On the contrary, the technical capacity demonstrated by the perpetrator proves that he is a competent, conscious, and fully responsible legal subject for his actions, so there is no room for doubt about the fulfillment of the capacity for accountability element in this case.

No excuse or justification can eliminate the perpetrator's criminal responsibility in this case. Force majeure or over majeure, as stipulated in Article 42 of the National Criminal Code, requires the existence of unbearable pressure so that the perpetrator has no other choice but to commit a prohibited act, while in this case, the perpetrator acted of his own free will with the sole motivation being financial gain. The defense of compulsion, as referred to in Article 34 of the National Criminal Code, is also irrelevant because the requirement of an immediate unlawful attack or threat is not completely met. This case also does not fulfill any of the justification requirements as stipulated in Articles 31-35 of the National Criminal Code because the perpetrator's actions were not carried out in the public interest, not based on a legitimate official order, and not in any emergency. The elimination of all possible excuses and justifications makes the perpetrator's criminal responsibility full, complete, and unavoidable, so that the perpetrator can be prosecuted based on a layered charge that combines Article 334 of the National Criminal Code as the primary charge, Article 35. Article 36 of the ITE Law, as a subsidiary charge, and Article 492 of the National Criminal Code on fraud are a safety net if the cyber technical elements are deemed insufficiently proven in court.

3.2 Legal Analysis of Regulations and Comparison of Related Articles: *Phishing* and *Social Engineering*

Cybercrime in the form of phishing continues to increase along with the widespread use of information technology and the digitalization of transactions in Indonesia. This method is generally carried out through social engineering, utilizing electronic media, such as email, messaging apps, and fake websites, to obtain victims' sensitive information, such as identity cards, passwords, and OTP codes. Phishing is not yet specifically defined as a stand-alone offense under Indonesian criminal law. However, the elements of the act are essentially reflected in various laws and regulations governing the misuse of electronic systems, misleading information, personal data protection, and digital transaction security.

The regulation most frequently used to prosecute phishing practices is Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024. Within the framework of the ITE Law, phishing can be linked to provisions regarding unauthorized access, manipulation of electronic systems, and the dissemination of false information that is detrimental to consumers. Article 28, paragraph (1), for example, can be applied when the perpetrator uses a fake identity or website to cause material losses. In addition, Article 36 is present to strengthen the basis for criminal liability if the actions referred to in Articles 30 to 34 cause losses to others. Therefore, in law enforcement practice, phishing cases usually do not stand on a single article, but are built through a combination of several interrelated provisions.

Not only Law Number 11 of 2008, but the 2024 amendment to the Electronic Information and Transactions Law also demonstrates efforts to adapt the law to developments in the digital space. Regulations regarding electronic certification, digital identity, and the use of certified electronic signatures, particularly for high-risk transactions, are crucial in the context of phishing prevention. These provisions essentially strengthen the authentication and verification processes in electronic transactions. The stricter the verification process, the less likely perpetrators are to use fake identities or create fake websites that mimic official platforms.

The strong link to phishing is also evident in Law Number 27 of 2022 concerning Personal Data Protection. This is understandable, as the primary goal of phishing is generally not only to deceive victims but also to obtain personal data for later misuse. The Personal Data Protection Law provides more comprehensive regulations regarding the types of personal data, the rights of data subjects, the obligations of data controllers and processors, and sanctions for data protection violations. Therefore, when phishing targets a victim's identity data, financial information, or personal profile, the act is no longer simply viewed as electronic fraud but also as a violation of the right to privacy and personal data protection.

[4] On a more operational level, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions places Electronic System Operators in a crucial position. This regulation requires operators to ensure the reliability, security, and sustainability of the electronic systems they manage. These obligations include implementing risk management, periodic audits, and governance that prioritizes data protection. In the context of phishing, this provision demonstrates that mitigation is not sufficient simply by criminalizing perpetrators. Prevention also depends on the extent to which system operators are able to close security gaps that can be exploited to commit digital fraud. Similar strengthening is evident in the electronic commerce sector. Through Government Regulation Number 80 of 2019 and Minister of Trade Regulation Number 31 of 2023, digital businesses are required to comply with the principles of transparency, business legality, complaint mechanisms, and a prohibition against misleading

promotions. This regulation is relevant because phishing practices often involve disguising business actors' identities, offering fictitious promotions, or directing consumers to fake transaction links. Therefore, the legal regime for electronic commerce plays a role in protecting consumers from various forms of digital fraud.

[5] In the financial services sector, phishing prevention has received more technical support through regulations from the Financial Services Authority (OJK). Regulations regarding the implementation of two-factor authentication (2FA), the provision of complaint channels, strengthening cyber resilience, and anti-fraud strategies demonstrate that customer protection is positioned as part of the obligations of financial service providers. This approach is crucial because the financial sector is a primary target for phishing, particularly when perpetrators attempt to gain access to accounts, banking applications, or customer credentials. Therefore, sectoral regulations in the financial services sector significantly contribute to strengthening risk prevention and mitigation. Although various legal instruments are available, phishing prevention in Indonesia is not yet fully effective. The main problem lies not merely in the lack of regulations, but in the fact that regulations are scattered across various legal regimes. As a result, law enforcement officials often have to piece together elements of a crime from several different provisions to construct a coherent indictment. This situation opens up considerable room for interpretation and can impact the consistency of law enforcement, particularly when proof relies heavily on electronic evidence and the ability of authorities to link the modus operandi to the elements of the alleged crime.

[6] In terms of substance, Indonesian positive law actually provides a basis for prosecuting the misuse of electronic systems and breaches of personal data. However, existing regulations do not explicitly define the currently emerging forms of phishing, such as credential harvesting, business email compromise (BEC), domain forgery, and OTP interception. The absence of more specific formulations does not necessarily create a legal vacuum, but rather indicates that the development of cybercrime methods is moving faster than the development of the norms governing them. In situations like this, law enforcement ultimately relies heavily on the interpretation of general provisions.

Another issue that requires attention is the incompleteness of implementing regulations for several provisions in the 2024 revision of the ITE Law. Although several supporting regulations are already in place, certain aspects still require further regulation, particularly those related to electronic certification providers, child protection in the digital space, and administrative sanction mechanisms. Without adequate implementing regulations, norms formulated at the legislative level risk being difficult to consistently implement at the technical and administrative levels. Based on this description, it is clear that Indonesia's legal framework for responding to phishing is essentially in place and sufficient as an initial basis for mitigation. Its main strength lies in the existence of regulations spread across various sectors, from cybercrime law, personal data protection, e-commerce, and financial services. However, a prominent weakness is the lack of a clear and integrated formulation of phishing as a specific offense. Therefore, future legal reforms need to be directed at harmonizing regulations, accelerating the formation of implementing regulations, and formulating more specific norms for various phishing methods, so that legal certainty and public protection can be more effectively realized.

Within the scope of cyber-criminal law (*cybercrime*) in Indonesia, phishing and social engineering are two related crimes, but have different levels of severity. Normatively, phishing *is* constructed as a technical act of manipulating electronic

systems, while social engineering focuses on the aspect of psychological manipulation. Based on Law No. 1 of 2024, phishing practices *are* generally charged using Article 35 concerning the manipulation of electronic information or documents to make it appear as if it were authentic data. This is often linked to Articles 30 to 32 concerning illegal access and unauthorized transmission of data.[7]On the other hand, the social engineering aspect, which contains elements of deception to mislead someone, it is more appropriate to use Article 28 paragraph (1) of the ITE Law regarding the dissemination of false information that results in consumer losses in electronic transactions.

A further comparison emerges when viewed with the recently enacted Law No. 1 of 2023 (New Criminal Code). If the ITE Law functions as a *Special Law i*n the digital sphere, the New Criminal Code, through Article 492 concerning fraud, provides a legal basis for aspects of social engineering that use a series of lies to induce others to hand over goods or data, as well as Article 391, which explains document forgery. The fundamental difference lies in the proof; the phishing article is a trap. In the ITE Law, proof is required of the existence of technical disruptions to the electronic system, whereas in social engineering. The New Criminal Code places greater emphasis on the causal relationship between the perpetrator's lies and the victim's negligence. This harmonization demonstrates that law enforcement is no longer a single entity, but rather an accumulation of articles on data manipulation and articles on conventional fraud that have been transformed.

In addition to the regulations mentioned above, the connection between these two methods can be considered a violation of a person's right to privacy, making Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) crucial. In this context, phishing is no longer only seen as an instrument of fraud, but also a criminal act of obtaining personal data by illegal means. If phishing and social engineering If the act is carried out to collect someone's identity or financial information, the perpetrator can be prosecuted under the criminal provisions of the Data Protection and Data Enforcement Law, which has specific sanctions related to data misuse. Thus, the synchronization of the ITE Law, the Data Protection and Data Enforcement Law, and the New Criminal Code creates a multi-layered legal framework that allows law enforcement to address the full scope of the crime, from the initial psychological engineering stage to the execution of data theft using complex electronic systems.

3.3 Efforts to Protect Victim Data in Criminal Acts: *Phishing* and *Social Engineering*

Phishing and social engineering are not being ignored by the government. As similar cases increase and develop, several efforts are being made to protect victims' data at various stages of the process. These efforts begin with preventive measures, namely, strengthening security systems and educating users. In the cybercrime landscape, preventive measures are the frontline in mitigating the risk of personal data leaks. Technically, the implementation of *Multi-Factor Authentication* (MFA) is a crucial standard for creating a double layer of security that makes unauthorized access difficult, even if the perpetrator has mastered a single credential. However, given the psychological manipulation nature of social engineering, system security must go hand in hand with customer legal literacy. Banking institutions like BCA urge customers to maintain the confidentiality of their PINs, OTPs, and other personal information *password*, until *appli token key*not just a technical procedure, but a form of fulfilling the obligation to maintain the principle of prudence*(duty of care)*Legally, this aligns with the obligation of electronic system administrators to maintain data integrity as stipulated in Law No. 1 of

2024 (Second Amendment to the ITE Law) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), where failure to protect data can result in administrative and civil sanctions.

Beyond preventive measures, responsive efforts also include investigations and synergy between relevant institutions. If a phishing incident has occurred, swift and measured responsive measures are crucial in limiting further losses. Banking institutions are required to conduct internal investigations to trace the flow of funds and detect system vulnerabilities exploited by the perpetrators. However, these investigations cannot stand alone; they require intersectoral collaboration with relevant authorities. Based on the nature of cybercrime, the involvement of the Ministry of Communication and Digital (formerly Kominfo) is vital in its capacity to terminate access.*(takedown)*to the site*p hissing* or fake accounts, as well as coordination with law enforcement officials for the forensic process *digital* responsive step is a manifestation of the responsibility of electronic system organizers to immediately provide notification and mitigation steps within 3 x 24 hours after a failure in personal data protection occurs, in accordance with the mandate of the PDP Law.

The government can also view the situation from the victim's perspective; therefore, victim recovery efforts are needed, particularly in restitution and dispute resolution. The aspect that is often most crucial for victims is the restoration of rights or restitution for financial losses suffered. Within the legal framework of consumer protection and banking, victims have the opportunity to pursue dispute resolution mechanisms through the bank's internal channels. *(Internal Dispute Resolution)* or externally through the Financial Services Authority (OJK) or the Alternative Dispute Resolution Institution (LAPS). *Phishing* And *Social Engineering* can be seen in the legal path, namely, focusing on proving whether the bank system was negligent or whether it was purely user error *(gross negligence).* If a weakness in the bank's security system is proven to have facilitated the cybercrime, customers have the right to demand a refund. This recovery effort is not simply about returning assets, but also about upholding justice for victims manipulated in a vulnerable digital ecosystem.

4. CONCLUSION

Based on the analysis carried out, the crime of *phishing* in digital banking services meets all elements of criminal liability. The perpetrator committed the crime by manipulating the electronic system and social engineering the victim. The perpetrator acted intentionally to gain illegal profits, had the capacity to take responsibility, and had no justification or justification for his actions. Therefore, law enforcement officials can prosecute the perpetrator to the fullest extent of the law.

Furthermore, the analysis shows that the legal framework in Indonesia has provided a legal basis for prosecuting crimes. The Electronic Information and Transactions Law, the National Criminal Code, and the Personal Data Protection Law regulate actions related to data manipulation, illegal access, and fraud. Law enforcement officials can apply these provisions in layers during the evidentiary process. Perpetrators can be subject to criminal sanctions in the form of imprisonment and/or fines in accordance with applicable regulations. However, these regulations are still scattered and do not yet address *phishing* as a special offense. This demonstrates the need for legal harmonization and reform to make law enforcement more effective.

In this regard, protection for victims of *phishing* requires a comprehensive approach. Banking institutions and related parties must implement preventative measures by strengthening security systems and increasing public digital literacy. Furthermore, relevant

institutions must be responsive, with swift handling and inter-agency coordination. Furthermore, victims have the right to redress through restitution and dispute resolution mechanisms. These mechanisms serve to ensure justice and define the boundaries of responsibility between banks and customers.

Thus, crime *phishing* is a multidimensional problem involving legal, technological, and user behavior aspects. Therefore, to overcome this, *s*trong law enforcement, adaptive regulations, and increased public protection and awareness are required. This integrated approach can provide legal certainty and optimal protection for digital service users.

5. BIBLIOGRAPHY

Website

Anti-Phishing Working Group. (2025). Phishing activity trends report: 4th quarter 2024. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

Khaerunnisa, R. (2026, January 25). BCA minta nasabah waspadai modus "phishing" melalui website palsu. ANTARA News. https://www.antaranews.com/berita/5375094/bca-minta-nasabah-waspadai-modus-phishing-melalui-website-palsu

National Institute of Standards and Technology. (n.d.). Phishing. In Computer Security Resource Center glossary. Retrieved April 27, 2026, from https://csrc.nist.gov/glossary/term/phishing

Otoritas Jasa Keuangan. (2021). Cetak biru transformasi digital perbankan. Otoritas Jasa Keuangan. https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx

Otoritas Jasa Keuangan Republik Indonesia. (2022). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Otoritas Jasa Keuangan. https://peraturan.bpk.go.id/Details/227376/peraturan-ojk-no-11pojk032022-tahun-2022

Otoritas Jasa Keuangan. (2023). Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum. https://www.ojk.go.id/id/regulasi/Pages/Layanan-Digital-oleh-Bank-Umum.aspx

Otoritas Jasa Keuangan. (2024). Peraturan Otoritas Jasa Keuangan Nomor 12 Tahun 2024 tentang Penerapan Strategi Anti Fraud bagi Lembaga Jasa Keuangan. https://ojk.go.id/id/regulasi/Pages/Penerapan-Strategi-Anti-Fraud-Bagi-Lembaga-Jasa-Keuangan.aspx

PT Bank Central Asia Tbk. (2025, November 27). Waspada penipuan phishing website palsu KlikBCA Bisnis! BCA. https://www.bca.co.id/id/informasi/awas-modus/2025/11/27/09/11/waspada-penipuan-phishing-website-palsu-klikbca-bisnis

Shaid, N. J. (2026, January 25). BCA ingatkan nasabah waspadai modus phishing lewat website palsu. *KOMPAS.com*. https://money.kompas.com/read/2026/01/25/220311826/bca-ingatkan-nasabah-waspadai-modus-phishing-lewat-website-palsu

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024

Article

Sitompul, J. (2024). Wajah Baru UU ITE. *JDIH Kemkomdigi*, 5. Retrieved April 25, 2026, from https://jdih.komdigi.go.id/artikel_hukum/artikel-hukum/t/artikel/85

Journal

Kaffah, A. F., & Badriyah, S. M. (2024). Aspek hukum dalam perlindungan bisnis era digital di Indonesia. *Jurnal Lex Renaissance*, *9*(1), 203–228. https://doi.org/10.20885/jlr.vol9.iss1.art10

Tampilan phising terhadap website Bank BCA. (n.d.). https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/293/276

Thenata, P. D. J., Susanto, R. J., Kurniawati, J. O., & Lee, J. C. (2025). Analisis Tanggung Jawab Hukum Terhadap Keamanan Perbankan dan Nasabah Dalam Kasus Phishing. *Cerdika Jurnal Ilmiah Indonesia*, *5*(4), 1641–1654. https://doi.org/10.59141/cerdika.v5i4.2628

View of Tanggung Jawab Bank terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk). (n.d.). https://www.ejournal.warmadewa.ac.id/index.php/juinhum/article/view/8318/5179

Law

Indonesia. (2008). Law Number 11 of 2008 concerning Electronic Information and Transactions.

Indonesia. (2024). Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Indonesia. (2023). Law Number 1 of 2023 concerning the Criminal Code

Indonesia. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Indonesia. Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems.

Indonesia. Law Number 27 of 2022 concerning Personal Data Protection.