Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 5 No. 6 (2025)

LEGAL ASPECTS OF CONSUMER PROTECTION AGAINST PHISHING CRIMES IN DIGITAL BUSINESS

Dahlan[1]*, Erniyanti[2], Henry Aspan[3], Etty Sri Wahyuni[4]
[1,3]Universitas Pembangunan Panca Budi, Medan, Indonesia
[2,4]Universitas Batam, Batam, Indonesia
E-mail: dln@gmail.com[1]*, eniyanti@univbatam.ac.id[2], henryaspan@yahoo.com[3], ettywahyunie@gmail.com[4]

Received	: 01 October 2025	Published	: 09 December 2025
Revised	: 10 October 2025	DOI	: https://doi.org/10.54443/morfai.v5i6.4677
Accepted	: 15 November 2025	Publish Link	: https://radjapublika.com/index.php/MORFAI/article/view/4677

Abstract

The development of digital business in Indonesia has brought significant impacts on the increase of cybercrime, particularly phishing. This research aims to analyze the legal aspects of consumer protection against phishing crimes in the context of digital business in Indonesia with a case study in Medan City. The research method used is normative juridical with statutory and case approaches. The research findings indicate that the legal framework for consumer protection against phishing crimes in Indonesia has been regulated in various regulations, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 27 of 2022 concerning Personal Data Protection. However, the implementation of legal protection still faces various obstacles, such as low digital literacy among the public, limited cyber law enforcement infrastructure, and complexity of evidence in phishing cases. This research recommends strengthening more specific regulations regarding phishing, increasing law enforcement capacity, and continuous public education.

Keywords: Consumer Protection, Phishing, Digital Business, Cybercrime, Indonesian Law

INTRODUCTION

The digitalization era has fundamentally transformed business transaction patterns in Indonesia. The development of information and communication technology has driven the transformation of conventional commerce toward electronic commerce (e-commerce), which offers greater convenience, efficiency, and accessibility for both consumers and business actors. Indonesia, as the largest digital economy in Southeast Asia, has experienced exponential growth in the e-commerce sector, supported by increased internet penetration and changes in consumer behavior that increasingly rely on online transactions to meet daily needs. Nevertheless, the rapid development of digital business also brings consequences in the form of increased cybercrime risks that threaten consumer security. Data from the National Cyber and Crypto Agency (BSSN) indicate a 70% increase in phishing cases compared to the previous year, with a total of more than 400 million cyber traffic anomalies detected throughout 2023. Phishing attacks have become one of the most prevalent forms of cybercrime targeting digital consumers in Indonesia, with financial losses estimated to reach billions of rupiah annually.

Phishing constitutes a form of cybercrime that employs social engineering techniques to obtain victims' sensitive information, such as login credentials, credit card data, or other personal information, by impersonating trusted entities through electronic communication. Phishing modus operandi continues to evolve alongside technological advances, ranging from sending fraudulent emails and creating fake websites to using malicious applications disguised as digital wedding invitations or other official documents. Medan City, as one of the digital economic centers in the Sumatra region, faces similar challenges regarding the increase in cybercrime cases. The rapid growth of digital startups, e-commerce, and digital financial services in Medan has created a dynamic digital business ecosystem, but has also increased vulnerability to phishing attacks targeting consumers in the region. This condition necessitates an in-depth study of the legal aspects of consumer protection in addressing the threat of phishing crimes in the digital business era. Based on this background, this study examines two principal issues: first, how is the legal regulation of consumer protection against phishing crimes in digital business in Indonesia; and second, how are the implementation and challenges of law enforcement against phishing crimes in protecting the rights of digital consumers. This research is expected to provide academic and practical contributions to the

development of a more comprehensive consumer protection legal framework in addressing cybercrime challenges in the digital era.

METHOD

This study employs a normative legal research method (juridical normative) with a statutory approach and case approach. The statutory approach is conducted by examining various regulations related to consumer protection and cybercrime in Indonesia, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and other relevant implementing regulations. The case approach is conducted by analyzing phishing crime cases that have occurred in Indonesia, particularly those relevant to consumer protection in digital business transactions. The research location is focused on Medan City, North Sumatra, as a representation of digital business dynamics and cybercrime outside Java Island, which possesses unique characteristics in terms of regional digital economic development. Research data sources consist of primary legal materials in the form of legislation, court decisions, and official government documents; secondary legal materials in the form of academic literature, scholarly journals, research findings, and legal doctrines; and tertiary legal materials in the form of legal dictionaries and encyclopedias. Data collection techniques are conducted through library research and systematic legal document searches. Data analysis is performed qualitatively using legal interpretation methods and logical reasoning to draw valid and scientifically accountable conclusions.

RESULTS AND DISCUSSION

1. Concept and Characteristics of Phishing Crimes in Digital Business

Phishing derives from the word "fishing," referring to criminals' attempts to "fish" for sensitive information from victims. In the cybercrime context, phishing is defined as a form of fraud that uses fake electronic messages to deceive victims into revealing personal information, security credentials, or other sensitive data. Phishing perpetrators generally impersonate trusted entities, such as banking institutions, e-commerce platforms, or government agencies, to build victim trust and lower their vigilance against actual threats. The main characteristics of phishing crimes in digital business include several fundamental aspects. First, the use of social engineering techniques that exploit human psychology, such as creating a sense of urgency, fear, or greed to encourage victims to act without critical thinking. Second, impersonation of trusted entity identities through the creation of fake websites, emails, or messages that visually resemble official communications from the imitated organization. Third, exploitation of technological vulnerabilities and victims' lack of digital literacy to launch increasingly sophisticated and difficult-to-detect attacks.

In Indonesia, phishing modus operandi has undergone significant evolution alongside technological development and changes in society's digital behavior. The most commonly found modus is reward-giving phishing, where perpetrators impersonate trusted organizations and direct victims to click on links that steal personal or financial information under the pretext of prize collection. Additionally, the use of malware and family crisis fraud has also become prevalent tactics in phishing attacks targeting Indonesian consumers. In the context of digital business in Medan City, phishing crimes have caused significant losses for consumers conducting e-commerce transactions, digital banking, and financial technology (fintech) services. Distinctive characteristics found include targeting users of local digital payment services, creating fake websites of marketplaces popular among Medan consumers, and sending WhatsApp messages or SMS containing malicious links disguised as transaction or goods delivery notifications. This condition is exacerbated by relatively low levels of digital literacy among the public, making them more vulnerable to increasingly sophisticated phishing attacks.

2. Legal Framework for Consumer Protection Against Phishing Crimes in Indonesia

Legal protection for consumers facing phishing crimes in Indonesia is regulated through several complementary legal instruments. Law Number 8 of 1999 concerning Consumer Protection (UUPK) serves as the primary foundation regulating consumer rights in general, including the right to security and comfort in transactions, the right to true, clear, and honest information, and the right to obtain compensation or damages in case of violations. Article 4 of UUPK explicitly states that consumers have the right to choose goods and services according to exchange value and conditions as well as promised guarantees, and the right to obtain advocacy, protection, and proper consumer protection dispute resolution efforts. In the context of electronic transactions, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) provides a more specific legal framework for addressing cybercrime, including phishing. Article 28 paragraph (1) of the ITE Law prohibits any person from intentionally and unlawfully disseminating false and misleading information

that results in consumer losses in electronic transactions. Violations of this provision may be subject to criminal sanctions in the form of imprisonment for a maximum of 6 (six) years and/or a fine of at most IDR 1,000,000,000 (one billion rupiah) as regulated in Article 45A paragraph (1). Furthermore, Article 35 of the ITE Law regulates the prohibition of manipulation, creation, alteration, elimination, or destruction of electronic information and/or electronic documents with the purpose of making such electronic information appear as authentic data. This provision is highly relevant to phishing modus operandi involving the creation of fake websites or counterfeit emails that resemble official communications from trusted entities. Sanctions for violators of Article 35 are regulated in Article 51 paragraph (1) of the ITE Law in the form of imprisonment for a maximum of 12 (twelve) years and/or a fine of at most IDR 12,000,000,000 (twelve billion rupiah).

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) represents an important milestone in strengthening digital consumer protection in Indonesia. The PDP Law comprehensively regulates the rights of personal data subjects, obligations of personal data controllers and processors, and sanctions for violations of personal data protection provisions. In the context of phishing crimes, the PDP Law provides legal protection for consumers who become victims of personal data theft by stipulating that any person who unlawfully obtains or collects personal data that does not belong to them with the intention of benefiting themselves or others, which may result in losses to the personal data subject, may be subject to imprisonment for a maximum of 5 (five) years and/or a fine of at most IDR 5,000,000,000 (five billion rupiah). Although the legal framework for consumer protection against phishing crimes in Indonesia is sufficiently comprehensive, several weaknesses require attention. First, the absence of a specific definition and regulation of phishing in Indonesian legislation, requiring law enforcers to use general provisions to prosecute phishing perpetrators. Second, the complexity of evidence in phishing cases involving electronic evidence and digital traces that are often difficult to track. Third, jurisdictional limitations in handling phishing cases that are transnational in nature. This condition necessitates regulatory updates that are more adaptive to developments in cybercrime modi operandi.

3. Implementation of Legal Protection and Law Enforcement Challenges

Implementation of legal protection for consumers who are victims of phishing crimes in Indonesia is carried out through various mechanisms, both preventive and repressive. Preventive efforts include education and socialization programs for the public regarding phishing dangers and methods of identifying cyber attacks, development of cybersecurity systems by digital business actors, and establishment of Computer Security Incident Response Teams (CSIRT) in various institutions. The government, through the National Cyber and Crypto Agency (BSSN), has initiated public awareness campaigns regarding basic cybersecurity practices and methods of protecting oneself from phishing threats. Repressive efforts are conducted through law enforcement against phishing crime perpetrators handled by the Indonesian National Police through the Cyber Crime Directorate (Dittipidsiber). In practice, law enforcement against phishing crimes faces various significant challenges. Data indicate that many reported phishing cases remain unresolved. This is caused by several factors, including difficulties in identifying and tracking perpetrators who frequently use anonymization techniques, limited resources and technical expertise of law enforcement officers in handling cybercrimes, and minimal reporting from victims due to low awareness and trust in the judicial system.

In Medan and its surrounding areas, implementation of legal protection against phishing crimes continues to face structural and cultural constraints. From a structural perspective, limited specialized cybercrime handling units at the regional police level and insufficient digital forensic facilities constitute major obstacles in the investigation process. From a cultural perspective, public awareness regarding personal data protection and online transaction security remains relatively low, contributing to high victimization rates from phishing attacks. Another challenge faced is jurisdictional complexity in handling transnational phishing cases. Phishing crime perpetrators often operate from abroad or use server infrastructure located in other countries, complicating law enforcement processes that require international cooperation. Indonesia has ratified the Convention on Cybercrime (Budapest Convention), which provides a framework for international cooperation in handling cybercrimes, but its implementation still requires strengthened inter-agency coordination and enhanced technical capacity. Regarding consumer loss recovery, compensation mechanisms for phishing victims remain suboptimal. Victimized consumers often face difficulties in obtaining restitution for financial losses suffered, whether through criminal or civil channels. This is caused by difficulties in identifying and locating perpetrators, limited assets that can be seized for victim compensation, and lengthy and costly judicial processes. Therefore, development of more effective and accessible alternative dispute resolution mechanisms for phishing crime victims is necessary.

4. Strategies for Strengthening Consumer Protection Against Phishing Crimes

Strengthening consumer protection against phishing crimes in digital business requires a holistic approach that integrates regulatory, technological, and educational aspects. From the regulatory aspect, updates and improvements to legislation that specifically define and regulate phishing crimes are necessary. Formulation of the phishing concept in the ITE Law or its implementing regulations will provide a stronger legal foundation and certainty in law enforcement. Additionally, consideration should be given to regulations regarding digital business actors' obligations to implement minimum security standards and effective phishing detection systems. From the technological aspect, implementation of anti-phishing technical solutions becomes an important component in consumer protection strategy. Measures that can be applied include use of multi-factor authentication (MFA), implementation of email security protocols such as DMARC, SPF, and DKIM to prevent domain spoofing, and development of artificial intelligence-based phishing detection systems that can identify and block attacks in real-time. E-commerce platforms and digital financial services also need to integrate stricter identity verification mechanisms and early warning systems for suspicious activities.

From the educational aspect, enhancing public digital literacy becomes key in phishing crime prevention efforts. Comprehensive education programs need to be implemented continuously through various channels, including formal education in schools and universities, public awareness campaigns through mass media and social media, and specialized training for vulnerable groups such as the elderly and communities with limited access to digital information. Educational materials should cover methods of identifying phishing signs, security practices in online transactions, and reporting procedures when becoming victims of cyber attacks. Institutional strengthening also becomes a critical aspect in consumer protection strategy. This includes enhancing the capacity and expertise of law enforcement officers in handling cybercrimes, establishing specialized cybercrime units in each police jurisdiction, and strengthening coordination among related institutions such as BSSN, Kominfo, OJK, and Bank Indonesia in supervising and handling phishing cases involving the financial sector. Cooperation with the private sector, particularly digital platforms and cybersecurity service providers, also needs to be enhanced to build a more comprehensive consumer protection ecosystem.

Specifically for Medan and North Sumatra, consumer protection strengthening strategies need to consider local characteristics regarding digital technology usage patterns and community literacy levels. Collaboration among local government, educational institutions, technology communities, and local digital business actors becomes important in building collective awareness and capacity to address phishing threats. Establishment of regional communication and coordination forums in handling cybercrimes can be a strategic step to enhance consumer protection effectiveness at the regional level.

CONCLUSION

Based on the research findings and discussion presented, the following conclusions can be drawn. First, the legal framework for consumer protection against phishing crimes in digital business in Indonesia has been regulated through various complementary legal instruments, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning ITE, and Law Number 27 of 2022 concerning Personal Data Protection. Article 28 paragraph (1) and Article 35 of the ITE Law serve as the primary foundation in handling phishing crimes, with sufficiently severe criminal sanction threats. Nevertheless, the absence of a specific definition and regulation of phishing in Indonesian legislation constitutes a weakness that needs to be addressed through regulatory updates. Second, implementation of legal protection for consumers who are victims of phishing crimes in Indonesia, particularly in Medan City, continues to face various obstacles that impede its effectiveness. Structural constraints include limited specialized cybercrime handling units, insufficient digital forensic facilities, and evidentiary complexity in phishing cases. Cultural constraints include low public digital literacy and minimal awareness regarding personal data protection. Jurisdictional challenges in handling transnational phishing cases and limited compensation mechanisms for victims also constitute problems requiring comprehensive handling.

Based on these conclusions, this study recommends several strategic measures. First, updates to the ITE Law are necessary by formulating a specific definition and regulation of phishing to provide legal certainty in law enforcement. Second, strengthening law enforcement officer capacity through specialized cybercrime handling training and provision of adequate digital forensic facilities. Third, implementation of massive and continuous digital literacy education programs involving all stakeholders. Fourth, development of more effective and accessible alternative dispute resolution mechanisms for phishing crime victims. Fifth, strengthening international cooperation in handling transnational phishing crimes through optimal implementation of the Budapest Convention and other bilateral/multilateral agreements.

REFERENCES

Anti-Phishing Working Group. (2024). Phishing Activity Trends Report Q2 2024. Retrieved from https://apwg.org/trendsreports/

Arifin, R., Kambuno, J. A., Waspiah, & Latifiani, D. (2021). Protecting the consumer rights in the digital economic era: Future challenges in Indonesia. Jambura Law Review, 3(3), 135-160.

National Cyber and Crypto Agency. (2024). Laporan Tahunan Keamanan Siber Indonesia [Indonesian Cybersecurity Annual Report]. Jakarta: BSSN.

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.

Hamzah, A. (2005). Aspek-aspek pidana di bidang komputer [Criminal aspects in the computer field]. Sinar Grafika.

Indonesia Anti-Phishing Data Exchange. (2024). Monthly number of phishing attacks recorded in Indonesia in 2023. Statista. Retrieved from https://www.statista.com/statistics/1411333/indonesia-monthly-number-of-phishing-attacks/

Irawan, F., Habsy, M., & Hosnah, A. (2025). Pertanggungjawaban pidana pelaku phishing dan efektivitas penegakan hukum berdasarkan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Jurnal Komputer, Informasi dan Teknologi, 5(2), 11.

Kadir, M. Y. A., Arifin, M., Disantara, F. P., Mac, Thuong, T. H., & Nutakor, B. S. M. (2024). The reform of consumer protection law: Comparison of Indonesia, Vietnam, and Ghana. Jurnal Suara Hukum, 6(2), 255-278.

Lasmadi, S. (2014). Pengaturan alat bukti dalam tindak pidana dunia maya. Jurnal Ilmu Hukum, 2(4).

Mansur, D. M. A., & Gultom, E. (2005). Cyber law: Aspek hukum teknologi informasi [Cyber law: Legal aspects of information technology]. PT Refika Aditama.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 132, 103387.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce menurut peraturan perundang-undangan di Indonesia. Jurnal Rechts Vinding Media Pembinaan Hukum Nasional, 12(2), 261-279.

Republic of Indonesia. (1945). Constitution of the Republic of Indonesia 1945 [Undang-Undang Dasar Negara Republik Indonesia Tahun 1945].

Republic of Indonesia. (1999). Law Number 8 of 1999 on Consumer Protection [Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen]. State Gazette of the Republic of Indonesia Year 1999 Number 22, Supplement to the State Gazette of the Republic of Indonesia Number 3821.

Republic of Indonesia. (2008). Law Number 11 of 2008 on Electronic Information and Transactions [Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik]. State Gazette of the Republic of Indonesia Year 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843.

Republic of Indonesia. (2016). Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions [Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik]. State Gazette of the Republic of Indonesia Year 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952.

Republic of Indonesia. (2022). Law Number 27 of 2022 on Personal Data Protection [Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi]. State Gazette of the Republic of Indonesia Year 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820.

Shaik, D., & Poojasree, V. (2021). Consumer protection in e-commerce: A legal and compliance framework in the digital market. In Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020) (pp. 18-23).

Sidobalok, J. (2014). Hukum perlindungan konsumen di Indonesia [Consumer protection law in Indonesia]. Citra Aditya Bakti.

SOCRadar. (2024). Indonesia Threat Landscape Report 2024. Retrieved from https://socradar.io/wp-content/uploads/2024/08/SOCRadar-Indonesia-Threat-Landscape-Report-2024.pdf

Statista. (2024). Estimated annual cost of cyber crime in Indonesia from 2018 to 2028. Retrieved from https://www.statista.com/forecasts/1411153/indonesia-cost-of-cyber-crime

Subekti, R. (2001). Hukum perjanjian [Contract law]. Intermasa.