JOURNAL OF LEGAL AND SOCIAL CHANGES
Scientia Plus Corp
P-ISSN: 00000
E-ISSN: 00000

# Juridical Analysis of Phishing Prevention in the Financial Institution Sector

**Muhammad Fadhooil Bagus Perdana[1], Moch Zulfa Nur Vais[2], Muhammad Tsalas Fahmi Al-Hakim[3], Muhammad Ranadhif Al-Fairuz[4], Muhammad Daffa Muhaimin[5], Muhammad Zidane Adjiasvino[6]**

[123456]Faculty of Law and Political Science, Muhammadiyah University of Surakarta, Sukoharjo, Central Java, 57169, Indonesia
*C100230280@student.ums.ac.id

**Article**

**Keywords:**
Phising; Financial Institutions; Siber Crime; Online Financial Services; OJK

**Article History**
Received: Jan 9, 2026;
Reviewed: Apr 16, 2026;
Accepted: Apr 30, 2026;
Published: May 1, 2026;

**Abstract**

Phishing crimes are becoming increasingly prevalent as more people use digital technology and online financial services, but the implementation of data protection regulations faces constraints in terms of monitoring and enforcement capacity in the field. This research was conducted using a normative juridical method with a descriptive research nature that relies on an analysis of laws and regulations, expert opinions, and sectoral regulations such as the ITE Law, the Personal Data Protection Law, the Criminal Code, and provisions from the Financial Services Authority (OJK) and Bank Indonesia. The research problem formulation covers two main points: (1) What are the legal regulations for phishing crimes, and (2) How effective is the implementation of legal provisions in efforts to combat phishing crimes in Indonesia. The results of the study indicate that normatively, regulations are quite comprehensive through a combination of criminal regulations, personal data protection provisions, and electronic system security standards in the financial services sector. However, in practice, law enforcement still faces several obstacles such as limited digital forensic capabilities, difficulties in obtaining cross-border electronic evidence, weak coordination between relevant institutions, and low levels of digital literacy in the community. In addition, financial institution security standards are not yet fully uniform, so there are still gaps that can be exploited by phishing perpetrators. This study concludes that the effectiveness of phishing countermeasures is suboptimal because the implementation of the legal formula has not been as robust as its normative concept. Therefore, a more comprehensive approach is needed through increased investigator capacity, updated digital forensic procedures, tightened security standards for electronic

system providers, strengthened inter-agency coordination, and regular public education to ensure more effective phishing prevention and enforcement efforts and protect users of digital financial services.



## INTRODUCTION

At this time, information and communication technology is developing very quickly, making the world infinite, space, time and distance so that it is able to change a person's way of life and a new order of life[1]. People are not only using information and communication technology as a tool to search for information, but also as a means to expand social networks and seek popularity. Platforms like Facebook, Twitter, Instagram, Snapchat, and more are becoming places where people connect, share experiences, and create their digital identities. In this way, crime also develops and modern crimes are born[2].

One of them is phishing, according to Chiew et al. The word "phishing" comes from the word "fishing," because phishing operations are comparable to fishing in which the attacker "lures" the victim by using "bait" and "fishing" for the victim's personal or confidential information. Phishing is a form of online fraud in which perpetrators try to obtain confidential or sensitive information from victims by posing as a trusted entity. This modus operandi can occur through emails, fake websites, or fake messages sent through various platforms. By taking advantage of the victim's attraction or interest, phishing perpetrators create an illusion of security or self-interest to trick them into inadvertently providing valuable information[3]. The phenomenon of phishing is not only a local threat, but also spreads globally along with technological developments. In the Indonesian context, cybercrime is a growing problem. One of the most common forms of cybercrime in Indonesia is phishing. Perpetrators of this crime often use fake emails or websites to trick people into providing confidential information such as usernames, passwords, or even credit card numbers[4].

This study aims to evaluate the legal aspects of the phenomenon of data leakage due to phishing in Indonesia, by examining the extent to which existing regulations,

[1] Aryono, & Barkhuizen, J. (2021). Criminal Law Enforcement of Phising Attacks on Online Banking Services. 2nd International Conference of Health, Science and Technology, 360–363.
[2] Wibisono, C. S., & Mahanani, A. E. E. (2023). Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial ( Twitter ). JURNAL HUKUM, POLITIK DAN ILMU SOSIAL (JHPIS), 2(2), 125–146.
[3] Az-zahra, I., & Labib, Z. M. (2024). Perlindungan Hukum bagi Nasabah dalam Kasus Phising dan Siber Perbankan di Indonesia. Yurisprudentia: Jurnal Hukum Ekonom, 10(2), 405–425.
[4] Apriani, R. (2025). The Legal Protection Regarding Consumer Losses in Banking Transactions Caused by Phishing. PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM, 24(1), 733–748.

especially the ITE Law and regulations related to personal data protection, are able to respond to contemporary challenges in the cyber world. The main focus is on understanding the legal implications of user privacy violations, as well as how the norms and principles of human rights protection, particularly the right to privacy, are positioned in national cyber policies[5].

## METHOD

The approach method applied in this study is a normative juridical approach method, the research specification used is descriptive. Conclusions from the results of this study were drawn by qualitative normative analysis method. Normative is to use only secondary data sources, namely laws and regulations, legal theories and the opinions of scholars, especially. Qualitative because it is a data analysis process without using formulas and figures derived from the information from the literature, namely data taken from related agencies and the results of observations in research conducted with the problem discussed[6].

## RESULTS AND DISCUSSION

### What is the legal regulation against the crime of phishing?

Phishing crime is a form of electronic fraud that uses social engineering to obtain sensitive victims' data, thereby posing a threat to public privacy and financial security. Legal regulations against phishing are basically spread across several norms. General criminal provisions on fraud as well as special rules in the field of information technology. In Indonesia, the Electronic Information and Transaction Law (UU ITE) is often used as the basis for cracking down on phishing actions that use electronic media. Some researchers consider that the existing provisions still need sharpening in order to specifically ensnare modern phishing techniques[7]. One of the regulatory challenges is the legal vacuum where the word phishing itself is not always explicitly mentioned in the old law, so law enforcement officials interpret phishing as an act of fraud or misuse of electronic information. This interpretive approach allows for prosecution, but it also leaves room for inconsistent handling of cases between jurisdictions. Hence there have been calls for more detailed regulation, including definitions, criminal elements, and specific sanctions for phishing. Research comparing enforcement practices noted the need for harmonization of norms at the national level[8].

Personal data protection regulations are an important instrument to reduce the impact of phishing, as many attacks aim to access data protected by data protection rules. With the advent of more modern data protection laws, victims have a legal basis to sue and regulators have the authority to impose

[5] Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia ( APJII ) tahun 2023 , lebih dari 215 juta penduduk telah terhubung. 4(1).
[6] Banjarnahor, A. C., Priyana, P., Karawang, U. S., Hukum, F., Karawang, U. S., & Hukum, F. (2022). KASUS PHISING KREDIVO. 6(1).
[7] Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. 5(1), 19–24.
[8] Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web tindakan dan perbuatan hukum yang nyata . Secara yuridis dalam hal ruang cyber. 6(1), 226–241.

administrative sanctions on electronic system operators. However, the implementation of data protection rules faces obstacles in the capacity of supervision and enforcement in the field. Therefore, a number of authors emphasize the combination of administrative and criminal sanctions for the effectiveness of prevention[9].

At the international level, the review of phishing regulations highlights countries that have already developed a package of anti-phishing laws, including norms on service provider liability, cross-border cooperation, and victim recovery mechanisms. This international experience is important for designing domestic policies because cybercrime is transnational in nature and perpetrators often operate from different jurisdictions. Countries that have clear regulations against electronic fraud and a quick take-down mechanism tend to be more effective at suppressing phishing activities. Comparative studies also recommend increased international cooperation and electronic evidence exchange[10].

The role of financial institutions and regulators in the financial services sector is key because many phishing targets bank and e-wallet customers; Therefore, sectoral rules force banks to implement system security standards and incident reporting obligations. OJK and banking regulations require banks to organize electronic transaction security and provide a mechanism for compensation or settlement in the event of fraud due to bank negligence. However, the practice of handling victim claims still shows inconsistencies, so stricter guidelines for handling claims are needed. Research in the banking sector suggests strengthening technical and procedural security obligations for financial service providers[11].

Law enforcement against phishing perpetrators also faces technical difficulties: digital evidence is often scattered, encrypted, or on foreign servers, so the investigation process requires digital forensic capacity and international cooperation. The police and related authorities need to improve forensic competence and accelerate the mutual legal assistance (MLA) mechanism to obtain evidence abroad. In addition, regulations need to regulate procedures for handling electronic evidence so that forensic results can be accepted as strong evidence in court. Empirical studies show that increasing the capacity of investigators and harmonizing forensic procedures increases the resolution rate of phishing cases[12].

Prevention aspects through digital education and the security obligations of system operators are also part of an effective regulatory framework; The law is not enough if people remain vulnerable due to low digital literacy. Therefore, a good legal policy is usually accompanied by a user empowerment program, technical security standards for online platforms, and an obligation to report incidents by electronic system operators. Modern regulations combine hard law (sanctions) and soft law approaches (technical guidelines and literacy campaigns) for the best results. Several studies affirm the importance of a combination of legal policies and digital literacy programs[13].

However, a number of studies highlight the policy gap that emerges with new technologies. phishing that leverages AI or deepfakes that require updating norms to stay relevant in the face of more sophisticated fraud techniques. Legislators are required to develop flexible norms that can cover new technical variants without having to wait for lengthy legislation. In addition, the responsibility arrangements for platforms and technology service providers must be clearly formulated so that

---

[9] Irawati, H. P. (2024). Enforcement of Laws Against the Sale of Phishing Links for the Purpose of Personal Data Theft Based on the ITE Law. 3(4).
[10] Pavlyukova, E. V. (2020). Phishing attacks: legal regulation in the USA.
[11] Prayuti, Y., Lany, A., Marpaung, Y. E., & Lorentzon, E. (2024). Legal Protection of Consumers from Personal Data Security Risks , Threats of Fraud and Phishing ( Cybercrime ) in E-Wallet Payment Systems. Unram Law Review, 8(2).
[12] Aryono, & Barkhuizen, J. (2021). Criminal Law Enforcement of Phising Attacks on Online Banking Services. 2nd International Conference of Health, Science and Technology, 360–363.
[13] Apriani, R. (2025). The Legal Protection Regarding Consumer Losses in Banking Transactions Caused by Phishing. PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM, 24(1), 733–748.

mitigation and control efforts can be carried out quickly. Technology law researchers suggest the establishment of adaptive rules and security standards that are updated regularly.

Effective enforcement also requires remediation mechanisms for victims, including expedited procedures for account recovery, refunds, and compensation; Regulations that regulate victims' rights will increase public trust in the digital ecosystem. In addition, administrative mechanisms such as fines for organizers who neglect to maintain system security can complement criminal efforts against perpetrators. Restorative justice efforts are also discussed in some literature as an alternative settlement that focuses on recovering victims' losses. Policy studies confirm that the combination of criminal, administrative, and remedial sanctions strengthens the response to phishing[14].

One of the important aspects of phishing regulation is the accountability of banks as electronic system operators because many phishing attacks target customer accounts and banking data. Banks have a legal obligation to protect customer data, and failure to implement security measures can open up the opportunity for lawsuits if data is leaked due to phishing. Banking regulations and information technology provisions, such as the POJK and the ITE Law, explain how banks should establish security systems and reporting procedures. However, juridical analysis shows that although rules exist, in practice many banks have not been consistent in recovering customer losses after phishing incidents[15]. Therefore, regulations are needed that not only regulate prevention but also compensation mechanisms for phishing victims in the context of digital banking.

On the personal data protection side, special regulations such as the Personal Data Protection Act are particularly relevant to tackle phishing because phishing victims often lose sensitive personal data. The Personal Data Protection Law provides a legal basis for cracking down on the misuse of customer data obtained through phishing. In addition, state institutions such as the BSSN and the police cyber crime unit should strengthen collaboration to proactively crack down on phishing, including identification, blocking, and public education measures. Juridical research shows that phishing prevention strategies that are integrated between personal data regulation, criminal enforcement, and digital education are more effective than single regulations[16]. Thus, anti-phishing regulations should not be separated from data protection policies because the two are interrelated in maintaining citizens' digital security.

In conclusion, legal regulation of phishing crimes must be multi-dimensional: combining criminal provisions, personal data protection, banking sector obligations, digital forensic capacity, and prevention programs through literacy. Harmonization between rules, updating norms to deal with new techniques, and strengthening international cooperation are key to long-term effectiveness. In addition to establishing norms, the implementation in the field of investigator capacity, technical guidelines, and organizer compliance determine the extent to which regulations are able to reduce phishing incidents. Recent literature recommends an integrated policy package that combines prevention, protection, prosecution, and partnership[17].

---

[14] Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach. Pancasila and Law Review, 6(1), 15–44.
[15] Tanonggi, J. T., Pusparini, I., Limbon, C. P., Thiffani, G., & Siagan, S. N. (2024). Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing. Indonesian Journal of Law, 1(6), 186–194.
[16] Maramis, A. V., Doodoh, M., & Lambonan, M. L. (2025). TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DALAM MENGATASI CYBERCRIME PADA KASUS PHISHING. Fakultas Hukum Unsrat, 14(5).
[17] Irawati, H. P. (2024). Enforcement of Laws Against the Sale of Phishing Links for the Purpose of Personal Data Theft Based on the ITE Law. 3(4).

**The Extent of the Effectiveness of the Implementation of Legal Provisions in Efforts to Overcome the Crime of Phishing in Indonesia**

Phishing crimes are becoming more prevalent as more and more people use digital technology and online financial services. In Indonesia, there are already various legal regulations such as the Electronic Information and Transaction Law (ITE), the Banking Law, the Personal Data Protection Law, as well as the rules in the Criminal Code (KUHP) and technical regulations from the Financial Services Authority (OJK) and Bank Indonesia. Even so, the implementation of this regulation in overcoming phishing still faces obstacles. Effectiveness can be seen from three aspects: adequate regulation, law enforcement capabilities, and its impact on prevention and enforcement. Regulation-wise, the existing rules are quite adequate[18]. The ITE Law provides a legal basis for acts of data manipulation, information theft, or unauthorized use of personal data. The Banking Law and OJK regulations strengthen customer protection through bank supervision and information technology risk management. In addition, the Personal Data Protection Act provides the latest legal framework for protecting personal data, which is often a prime target for phishing attacks[19].

The existence of this rule is a strong legal basis to deal with perpetrators and protect victims. Even so, law enforcement is still ineffective. Recent research shows that law enforcement officers are limited in digital forensic capabilities, investigative infrastructure, and evidence collection from electronic devices. The nature of phishing that uses digital anonymity, deceptive technology, and overseas servers makes the process of identifying perpetrators difficult. Many cases cannot be followed up until the prosecution process, so the deterrent effect has not been achieved. In addition, bureaucratic procedures between agencies such as the police, PPATK, OJK, and the Ministry of Communication and Information are often slow, making handling unresponsive[20]. In terms of institutional coordination, cooperation between authorities, financial institutions, and digital service providers is still ineffective. Quick actions such as blocking a bank account, removing a phishing site, or reporting a crime can prevent losses.

However, in practice, there is a delay in checking or a lack of coordination causes many cases to not be resolved in a thorough manner. Several studies emphasize the importance of cooperation between legal and technical operational measures to reduce phishing crimes[21]. Another factor that affects effectiveness is the low public understanding of the digital world. Many victims are deceived by not recognizing signs such as fake links, obscure messages, or requests for personal data. The law only takes effect after the crime has occurred, while prevention depends on the user's awareness. Educational efforts by the government, banks, and digital platforms have been carried out, but they are not evenly distributed. This makes

[18] Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. 5(1), 19–24.
[19] Ekawati, D., Haryanti, A., & Herdiana, D. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. SIGn Jurnal Hukum, 7(1), 133–151.
[20] Nur'aini, R. J., & Simanjuntak, M. (2025). PHISHING AWARENESS AND SECURITY CONCERNS : ANALYZING THE ROLE OF ANTI-PHISHING KNOWLEDGE AND INTERNET. Jur. Ilm. Kel. & Kons., 18(2), 121–133.
[21] Sulistyo, A. D., Wicaksono, B. D., Saputra, R. N., & Ramadhani, R. (2024). Strategi Penanggulangan Serangan Phishing di Media Sosial. 385–396.

phishing prevention more dependent on non-legal factors, while new legal aspects play a role in the stage of handling and recovering losses[22]. In financial institutions, banks' internal protection mechanisms such as how to detect suspicious actions, layered security systems, and refund policies are an important part of efforts to prevent phishing actions.

Research shows that the combination of law enforcement and improvement of banks' internal policies yields quite good results in reducing emerging risks. However, the way to implement this policy still differs between banks, so the level of protection for customers is not always the same[23]. In general, the implementation of legal regulations to prevent phishing in Indonesia is quite complete normatively[24], but it is not yet effective in real terms. This means that the existing rules are adequate, but their implementation has not been able to significantly reduce the number of cases (Yustitiana, 2021)[25]. Several factors such as technical difficulties, lack of cooperation between institutions, limited law enforcement resources, and low digital capabilities of the community are the main obstacles in efforts to increase effectiveness[26]. Therefore, improvements are needed in the application of the law, the capabilities of the apparatus, faster coordination between agencies, international cooperation in investigations, and broader digital education so that prevention can run well[27].

## CONCLUSION

Digital fraud through phishing links is a criminal act as regulated in Article 378 of the Criminal Code. The punishment for digital fraud through phishing links is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 11 of 2008 concerning Information and Electronic Transactions[28]. Depending on what results are obtained from digital fraud through the phishing link Financial losses, identity theft, loss of personal information, stress and trauma that can damage physical and mental health, as well as operational disruption for individuals or corporate entities are just some of the serious consequences that phishing can have for its victims[29].

---

[22] Souhoka, B. A., Fadillah, R. A., Fathan, M., Meldiansah, R., Mutakin, M. I., & Fauziyah. (2025). Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook. JURNAL SISTEM INFORMASI GALUH, 3(1), 10–22.

[23] Lahagu, F., Erma, Z., & Nasution, R. (2025). Law Enforcement Against Cyber Crime in the Form of Phishing According to Law Number 1 of 2023 Concerning Criminal Code. 15(03), 869–878. https://doi.org/10.58471/justi.v15i03

[24] Mega, R., & Sari, P. (2025). Criminal Responsibility in Cybercrime : An Analysis of Phishing Crimes in Indonesia. 2(5), 49–55.

[25] Yustitiana, R. (2021). PELAKSANAAN PENGATURAN HUKUM TINDAK KEJAHATAN FRAUD PHISHING TRANSAKSI ELEKTRONIK SEBAGAI BAGIAN DARI UPAYA PENEGAKAN HUKUM DI INDONESIA DIKAITKAN DENGAN TEORI EFEKTIVITAS HUKUM. Jurnal Hukum Visio Justisia, 1, 98–126.

[26] Mega, R., & Sari, P. (2025). Criminal Responsibility in Cybercrime : An Analysis of Phishing Crimes in Indonesia. 2(5), 49–55.

[27] Aziz, L., Ardy, F., Istiqomah, I., Ezer, A. E., Neyman, S. N., & Linux, K. (2024). Phishing di Era Media Sosial : Identifikasi dan Pencegahan Ancaman di Platform Sosial. 4, 1–11.

[28] Sahfitri, A., Hukum, I., & Sumatera, U. (2024). PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. 6(2), 92–107.

[29] Fathonah, R., Cemerlang, A. M., Lampung, U., & History, A. (2025). Received: April 2025 Reviewed: April 2025 Published: April 2025. 11(9).

Additionally, phishing can result in losses such as status damage if victims' data is leveraged for malicious or illegal purposes, which can damage their reputation and reduce their credibility in the eyes of others, especially if they are public figures or companies. Then regarding the Liability for the crime of cyber crime phishing is regulated in the Electronic Information and Transaction Law, this is stated in Article 378 of the Criminal Code regarding fraud. Then it is also contained in Law Number 11 of 2008 concerning Information and Electronic Transactions and then Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions Article 35 jo Article 51 paragraph (1), Article 30 paragraph (3) jo Article 46 paragraph (3), Article 32 paragraph (2) jo. Article 48 paragraph (2). Then it is also contained in Law No. 27 of 2022 concerning Personal Data Protection Articles 66 and 67[30]. The regulation of criminal sanctions regarding the protection of personal data has differences in the imposition of minimum criminal sanctions, imprisonment and fines. In Indonesia, acts that violate Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) can be punished with a maximum prison sentence of 4 to 6 years and a maximum fine between IDR 4,000,000,000 to IDR 6,000,000,000,-. Compared to Indonesia, Malaysia regulates lower criminal sanctions, which are a maximum of 1 to 3 years. The Amendment to the Personal Data Protection Act (PDPA) 2010 (Act 709) in 2024 which is included in Act A1727 of the Personal Data Protection Act (Amendment) 2024 has significantly increased from RM 300,000 to RM 1 million[31].

To protect yourself from phishing attacks, the first step is to identify and implement the right cybersecurity solutions. This includes selecting effective tools and strategies in preventing and detecting phishing attacks. The second step is to design and execute a phishing attack prevention simulation, which aims to test the system's readiness and response to the threat. The third step is to analyze the impact after implementation and simulation of prevention, to understand the effectiveness of the measures taken and make the necessary adjustments to improve overall cybersecurity[32].

[30] Reyhan, E., & Gultom, P. (2025). PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG- UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. Lex Laguens: Jurnal Kajian Hukum Dan Keadilan, 3(3), 111–124.

[31] Cahyaningsih, R. D., Fauzan, A., Hasbi, S., & Winanti, A. (2025). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi : Studi Perbandingan Indonesia dan Malaysia Criminal Law Policy for Combating Phishing Crimes Through the Personal Data Protection Act : Compa. Abdurrauf Science and Society, 1(4), 800–811.

[32] Aziz, L., Ardy, F., Istiqomah, I., Ezer, A. E., Neyman, S. N., & Linux, K. (2024). Phishing di Era Media Sosial : Identifikasi dan Pencegahan Ancaman di Platform Sosial. 4, 1–11.

## REFERENCES

Anjheli, D. (2024). *Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia ( APJII ) tahun 2023 , lebih dari 215 juta penduduk telah terhubung*. *4*(1).

Apriani, R. (2025). The Legal Protection Regarding Consumer Losses in Banking Transactions Caused by Phishing. *PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM*, *24*(1), 733–748.

Aryono, & Barkhuizen, J. (2021). Criminal Law Enforcement of Phising Attacks on Online Banking Services. *2nd International Conference of Health, Science and Technology*, 360–363.

Az-zahra, I., & Labib, Z. M. (2024). Perlindungan Hukum bagi Nasabah dalam Kasus Phising dan Siber Perbankan di Indonesia. *Yurisprudentia: Jurnal Hukum Ekonom*, *10*(2), 405–425.

Aziz, L., Ardy, F., Istiqomah, I., Ezer, A. E., Neyman, S. N., & Linux, K. (2024). *Phishing di Era Media Sosial : Identifikasi dan Pencegahan Ancaman di Platform Sosial*. *4*, 1–11.

Banjarnahor, A. C., Priyana, P., Karawang, U. S., Hukum, F., Karawang, U. S., & Hukum, F. (2022). *KASUS PHISING KREDIVO*. *6*(1).

Cahyaningsih, R. D., Fauzan, A., Hasbi, S., & Winanti, A. (2025). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi : Studi Perbandingan Indonesia dan Malaysia Criminal Law Policy for Combating Phishing Crimes Through the Personal Data Protection Act : Compa. *Abdurrauf Science and Society*, *1*(4), 800–811. https://doi.org/10.70742/asoc.v1i4.283

Ekawati, D., Haryanti, A., & Herdiana, D. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. *SIGn Jurnal Hukum*, *7*(1), 133–151.

Fathonah, R., Cemerlang, A. M., Lampung, U., & History, A. (2025). *Received: April 2025 Reviewed: April 2025 Published: April 2025*. *11*(9).

Irawati, H. P. (2024). *Enforcement of Laws Against the Sale of Phishing Links for the Purpose of Personal Data Theft Based on the ITE Law*. *3*(4).

Lahagu, F., Erma, Z., & Nasution, R. (2025). *Law Enforcement Against Cyber Crime in the Form of Phishing According to Law Number 1 of 2023 Concerning Criminal Code*. *15*(03), 869–878. https://doi.org/10.58471/justi.v15i03

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). *Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia*. *5*(1), 19–24.

Maramis, A. V., Doodoh, M., & Lambonan, M. L. (2025). TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DALAM MENGATASI CYBERCRIME PADA KASUS PHISHING. *Fakultas Hukum Unsrat*, *14*(5).

Mega, R., & Sari, P. (2025). *Criminal Responsibility in Cybercrime : An Analysis of Phishing Crimes in Indonesia*. *2*(5), 49–55.

Muhammad, F. E., & Harefa, B. (2023). *Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web tindakan dan perbuatan hukum yang nyata . Secara yuridis dalam hal ruang cyber*. *6*(1), 226–241.

Nur'aini, R. J., & Simanjuntak, M. (2025). PHISHING AWARENESS AND SECURITY CONCERNS : ANALYZING THE ROLE OF ANTI-PHISHING KNOWLEDGE AND INTERNET. *Jur. Ilm. Kel. & Kons., 18*(2), 121–133.

Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach. *Pancasila and Law Review*, *6*(1), 15–44.

Pavlyukova, E. V. (2020). *Phishing attacks: legal regulation in the USA*.

Prayuti, Y., Lany, A., Marpaung, Y. E., & Lorentzon, E. (2024). Legal Protection of Consumers from Personal Data Security Risks , Threats of Fraud and Phishing ( Cybercrime ) in E-Wallet Payment Systems. *Unram Law Review*, *8*(2).

Reyhan, E., & Gultom, P. (2025). PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG- UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan*, *3*(3), 111–124.

Sahfitri, A., Hukum, I., & Sumatera, U. (2024). *PENIPUAN DIGITAL MELALUI TAUTAN PHISHING*. *6*(2), 92–107.

Souhoka, B. A., Fadillah, R. A., Fathan, M., Meldiansah, R., Mutakin, M. I., & Fauziyah. (2025). Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook. *JURNAL SISTEM INFORMASI GALUH*, *3*(1), 10–22.

Sulistyo, A. D., Wicaksono, B. D., Saputra, R. N., & Ramadhani, R. (2024). *Strategi Penanggulangan Serangan Phishing di Media Sosial*. 385–396.

Tanonggi, J. T., Pusparini, I., Limbon, C. P., Thiffani, G., & Siagan, S. N. (2024). Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing. *Indonesian Journal of Law*, *1*(6), 186–194.

Wibisono, C. S., & Mahanani, A. E. E. (2023). Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial ( Twitter ). *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL (JHPIS)*, *2*(2), 125–146.

Yustitiana, R. (2021). PELAKSANAAN PENGATURAN HUKUM TINDAK KEJAHATAN FRAUD PHISHING TRANSAKSI ELEKTRONIK SEBAGAI BAGIAN DARI UPAYA PENEGAKAN HUKUM DI INDONESIA DIKAITKAN DENGAN TEORI EFEKTIVITAS HUKUM. *Jurnal Hukum Visio Justisia*, *1*, 98–126.