Journal of Cyber Law and Information Security
Volume 1, Number 2, 2022

Regulating Phishing and Digital Impersonation in Indonesia: Assessing the Effectiveness and Limitations of the ITE Law

Muhammad Afif Kafandi[1*]

[1] Universitas Pembangunan Nasional "Veteran", Jakarta, Indonesia

Abstract

Article history:
Received: July 17, 2022
Revised: August 08, 2022
Accepted: October 04, 2022
Published: December 30, 2022

Keywords:
Consumer Protection, Digital Impersonation, ITE Law, Phishing, Regulatory Effectiveness.

Identifier:
Zera Open
Page: 95-114
https://zeraopen.com/journal/jclis

Phishing and digital impersonation have become significant cybercrime concerns in Indonesia because they exploit electronic transactions, institutional trust, and users' limited ability to verify digital identities. This study examines two main questions: to what extent the Electronic Information and Transactions Law (ITE Law) effectively regulates phishing and digital impersonation, and why these offenses urgently require legal assessment. Using a normative juridical approach, the study analyzes statutory provisions, legal concepts, scholarly literature, and selected public cases involving fake customer service accounts and phishing schemes. The discussion shows that Articles 28 paragraph (1), 30, 35, and 51 of the ITE Law provide a legal basis for addressing misleading information, unauthorized access, and manipulated electronic information. However, the law remains limited because phishing and digital impersonation are not expressly formulated as independent offenses, creating fragmented interpretation and evidentiary challenges. The study concludes that Indonesia needs clearer legal interpretation, stronger institutional coordination, and more preventive regulatory mechanisms to improve legal certainty, consumer protection, data security, and public trust in digital services.

*Corresponding author:
(Muhammad Afif Kafandi)

1. Introduction

The expansion of digital transactions in Indonesia has transformed how individuals communicate, bank, shop, and access public services. However, the same digital environment has also created opportunities for cyber-enabled fraud, particularly phishing and digital impersonation. Phishing usually operates by deceiving users into submitting confidential data, such as usernames, passwords, banking credentials, card numbers, or one-time password codes, through fake websites, false messages, imitation accounts, or fraudulent communication channels. Digital impersonation strengthens this method because the perpetrator does not merely send misleading information, but also performs a false identity by imitating trusted institutions, customer service channels, banks, marketplaces, or public authorities. In this context, the legal issue is not only whether the victim suffers financial loss, but also whether Indonesian cyber law can identify, classify, and punish the deceptive digital conduct that makes such loss possible.

Several public cases show that phishing and impersonation are no longer isolated technical incidents. Indonesian media reported that fake customer care accounts imitating bank identities were actively targeting customers on social media by responding to complaints, directing users to private WhatsApp communication, and exploiting panic during banking problems (Kusuma, 2021). Another example involved fake call center schemes targeting bank customers through WhatsApp profiles using institutional logos, business-account labels, and phishing pages designed to collect card and mobile banking credentials (Tanujaya, 2021). These cases demonstrate that phishing is often inseparable from impersonation, social

engineering, misuse of electronic systems, and the exploitation of public trust in digital service providers.

The Electronic Information and Transactions Law (ITE Law), particularly Law Number 11 of 2008 as amended by Law Number 19 of 2016, provides the main legal framework for addressing cybercrime in Indonesia. In phishing-related cases, several provisions may be relevant, including Article 28 paragraph (1) on false and misleading information causing consumer loss, Article 30 on unauthorized access, Article 35 on manipulation, creation, alteration, deletion, or destruction of electronic information or documents, and Article 51 on criminal sanctions related to manipulated electronic information. However, the effectiveness of these provisions remains debated because phishing is not expressly formulated as an independent offence in the ITE Law. Gulo et al. (2020) argue that phishing under the ITE framework still creates interpretive difficulties, particularly because not every phishing act can be easily fitted into Article 35 or Article 28 paragraph (1). Similarly, Putra (2021) emphasizes that phishing has legal ambiguity because the modus operandi involves deception, fake electronic information, and unauthorized acquisition of account access at the same time.

This ambiguity matters because the criminal construction of phishing may shift between fraud, unauthorized access, data manipulation, identity misuse, or consumer harm depending on the facts of each case. Indonesian legal scholarship has shown that cybercrime regulation often faces the difficulty of adjusting conventional criminal law concepts to conduct committed through electronic systems (Alfian, 2017). In the context of online fraud, Tantimin (2021) also notes

that the ease of digital transactions increases the risk of fraudulent conduct, including cases involving vulnerable perpetrators and victims. Meanwhile, studies on carding and electronic financial crime illustrate that the ITE Law can reach certain unauthorized uses of electronic data, but its provisions may not cover all actors and stages in complex cybercrime schemes (Adhi & Soponyono, 2021). These findings suggest that the ITE Law has normative value as a legal basis, yet its practical effectiveness depends on how precisely law enforcement can connect the act of impersonation, the fraudulent message, the unauthorized access, and the resulting loss.

The urgency of examining phishing and digital impersonation under the ITE Law lies in their significant implications for legal certainty, consumer protection, data security, and public trust in digital services. Unlike conventional fraud, phishing can be automated, rapidly replicated, and distributed across multiple digital platforms, while digital impersonation enables perpetrators to exploit the credibility of legitimate institutions. Consequently, victims often remain unaware that they are interacting with fraudulent actors until financial or data losses have occurred. Despite the existence of the ITE Law as the primary legal framework for addressing cyber-related offenses, its provisions remain broad and fragmented, raising concerns regarding its effectiveness in responding to increasingly sophisticated forms of cybercrime. This gap highlights the need for a more focused juridical assessment of the law's capacity to address these specific offenses. Therefore, this article evaluates the effectiveness of the ITE Law in regulating phishing and digital impersonation in

Indonesia, and critically examines the urgency of strengthening the regulatory framework in response to its limitations and the evolving nature of cybercrime.

2. Research Methods

This study uses a normative juridical research method to examine the regulation of phishing and digital impersonation under Indonesia's ITE Law. A normative approach is appropriate because the main objective of the study is to analyze legal norms, statutory provisions, doctrinal interpretations, and conceptual limitations within the existing regulatory framework. Rather than measuring the frequency of phishing cases empirically, this study focuses on how the law defines, classifies, and responds to phishing and digital impersonation as forms of cyber-related offenses.

The primary legal materials used in this study consist of Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 19 of 2016 as its amendment, and relevant provisions of the Indonesian Criminal Code where necessary, particularly those related to fraud and identity-related deception. These legal materials are examined to identify whether the existing provisions can adequately regulate phishing and digital impersonation, especially in relation to false information, unauthorized access, electronic data manipulation, and consumer loss. The study also uses secondary legal materials, including peer-reviewed journal articles, academic legal commentaries, and scholarly studies discussing cybercrime, phishing, online fraud, carding, and the enforcement of the ITE Law in Indonesia.

Reputable news reports are used only as supporting materials to illustrate concrete cases and factual phenomena, not as the main basis for legal interpretation.

The analysis is conducted through statutory, conceptual, and case-based approaches. The statutory approach is used to examine the scope and limitations of relevant provisions in the ITE Law. The conceptual approach is applied to clarify the legal meaning of phishing and digital impersonation, particularly because these acts may overlap with fraud, identity misuse, unauthorized access, and manipulation of electronic information. The case-based approach is used to connect legal norms with real-world examples of fake customer service accounts, fraudulent digital communication, and phishing schemes targeting banking customers.

Data analysis is carried out qualitatively through descriptive and prescriptive legal analysis. The descriptive analysis explains how the current legal framework regulates phishing-related conduct, while the prescriptive analysis evaluates whether the framework is sufficiently effective and what regulatory improvements may be required. The effectiveness of the ITE Law is assessed based on legal certainty, clarity of offense formulation, enforceability, victim protection, and the law's ability to respond to evolving cybercrime methods. This methodological design allows the study to answer two central questions: the effectiveness of the ITE Law in regulating phishing and digital impersonation, and the urgency of strengthening the regulatory framework in response to its limitations.

3. Results and Discussion

3.1. How Effective Is the Electronic Information and Transactions Law in Regulating Phishing and Digital Impersonation in Indonesia?

The Electronic Information and Transactions Law, particularly Law Number 11 of 2008 as amended by Law Number 19 of 2016, provides an important normative foundation for responding to phishing and digital impersonation in Indonesia. Although the law does not expressly use the terms "phishing" or "digital impersonation" as independent criminal categories, several provisions can be interpreted to cover the main legal elements of these offenses. Phishing commonly involves deceptive electronic communication, false representation, unauthorized acquisition of confidential information, and possible financial loss. Digital impersonation, meanwhile, usually involves the use of another person's or institution's identity, logo, account name, electronic address, or digital communication style to create a false sense of legitimacy. These acts can be connected to Article 28 paragraph (1), Article 30, Article 35, and Article 51 of the ITE Law, depending on the structure of the conduct and the evidence available.

Article 28 paragraph (1) is relevant because phishing frequently uses false and misleading information that causes consumer loss in electronic transactions. In fake bank customer service cases, perpetrators may pretend to represent a bank, respond to user complaints, and persuade victims to submit confidential credentials through WhatsApp, fake links, or imitation digital forms. This pattern reflects the core element of misleading electronic information because the victim is induced to believe that the communication is legitimate. Kusuma (2021) shows how fake customer care

accounts on social media exploited customer complaints by imitating banking service channels and redirecting victims to private communication. Similarly, Tanujaya (2021) illustrates the use of fake call center profiles and phishing pages to collect banking credentials. These cases indicate that Article 28 paragraph (1) can be applied when phishing is framed as false electronic information that causes consumer harm.

However, the effectiveness of Article 28 paragraph (1) is limited by the requirement to prove a connection between misleading electronic information and consumer loss. Phishing does not always occur in the form of a completed transaction. Sometimes the perpetrator only collects credentials, installs malware, or gains access to the victim's account before a financial transaction occurs. In such cases, the loss may not yet be visible, or the victim may suffer data exposure rather than immediate financial damage. Gulo et al. (2020) argue that phishing under the ITE Law creates interpretive challenges because the act may involve deception, data manipulation, unauthorized access, and electronic fraud at the same time. This makes the legal classification of phishing dependent on which element can be most strongly proven by investigators and prosecutors. As a result, the law has a functional basis for enforcement, but it does not yet provide a precise offense formulation.

Article 30 of the ITE Law is also relevant when phishing leads to unauthorized access into an electronic system. If a perpetrator uses stolen credentials to enter a victim's banking account, e-mail account, marketplace account, or mobile banking application, the conduct can be understood as access without right. This provision is important because phishing is not only a deception-based crime, but also a gateway to unlawful entry into electronic systems. Koto (2021) explains that

cybercrime under the ITE Law includes unlawful conduct committed through electronic systems, and unauthorized access is one of the central forms of cyber offending. In this sense, the ITE Law can respond to the post-phishing stage, particularly when the perpetrator has moved from deception to system intrusion.

Nevertheless, Article 30 may not fully address the preparatory and representational aspects of phishing. A perpetrator who creates a fake customer service account, sends deceptive messages, or designs a phishing page may not yet have entered the victim's system. The offense may still be in the stage of inducement or attempted data acquisition. If law enforcement relies only on unauthorized access, then the legal response may become reactive because it focuses on access after the victim's data has been used. This is problematic because phishing prevention requires legal tools that can address impersonation and deceptive data collection before larger harm occurs. Therefore, Article 30 is useful but incomplete when applied to phishing as a whole.

Article 35 is perhaps one of the most important provisions for digital impersonation because it prohibits unlawful manipulation, creation, alteration, deletion, or destruction of electronic information or electronic documents with the purpose of making such information appear authentic. This provision can cover fake websites, fake forms, altered digital identities, and manipulated electronic documents. Putra (2021) emphasizes that phishing often operates through a modus operandi in which false electronic information is presented as legitimate, causing victims to believe that they are interacting with a trusted party. In digital impersonation cases, the creation of an account or website that imitates a legitimate

institution may be legally understood as the creation or manipulation of electronic information to make it appear authentic.

The strength of Article 35 lies in its focus on authenticity. Digital impersonation is harmful precisely because it creates false authenticity. A fake bank account, fake official WhatsApp number, or fake payment page works because it visually and communicatively resembles a legitimate channel. From a normative perspective, Article 35 is therefore capable of capturing the identity-fabrication element in phishing. However, the limitation lies in the need to prove intent and the specific purpose of making electronic information appear authentic. Where the impersonation is subtle, temporary, or distributed through multiple accounts, proof may become difficult. In addition, the article does not specifically explain digital identity misuse, brand impersonation, or institutional impersonation as separate legal categories. This leaves room for inconsistent interpretation.

The ITE Law is also effective to the extent that it functions as a lex specialis for offenses committed through electronic systems. Alfian (2017) notes that cybercrime regulation in Indonesia is intended to strengthen legal control over crimes that develop through information technology. Compared to relying only on conventional fraud provisions in the Criminal Code, the ITE Law allows law enforcement to address the electronic nature of the offense, including electronic information, electronic documents, system access, and digital evidence. This is important because phishing cannot be fully understood as ordinary deception. It involves technological infrastructure, platform-based communication, and electronic traces that require cyber-specific legal interpretation.

Even so, the law's effectiveness is constrained by fragmentation. Phishing may be prosecuted through one provision if it is seen as false information, another if it is seen as unauthorized access, and another if it is seen as manipulation of electronic information. Adhi and Soponyono (2021), in discussing carding, show that cyber-enabled financial crimes often involve several stages and actors, making legal classification complex. This insight is relevant to phishing because one actor may create the phishing page, another may distribute the link, another may collect credentials, and another may withdraw funds. Fuad (2021) also shows that cyber-enabled financial crimes such as carding may involve stolen credentials, electronic transactions, and technical complexity that make investigation and proof more difficult. Therefore, phishing should not be analyzed only from the perspective of the final financial transaction, but also from the earlier stages of identity falsification, data acquisition, and unlawful preparation.

The effectiveness of the ITE Law is further limited by the relationship between criminal law and cybersecurity governance. Criminal provisions may punish perpetrators after the offense occurs, but phishing and digital impersonation also require prevention, early detection, public warning, and takedown mechanisms. Aulianisa and Indirwan (2020) argue that strengthening cybersecurity and cyber-resilience in Indonesia requires clearer legal and institutional arrangements. This argument is relevant because phishing does not only expose weaknesses in criminal law formulation, but also weaknesses in prevention systems. When fake accounts remain active, phishing links circulate widely, or victims do not know where to report

suspicious activity, the regulatory framework has not fully protected the digital ecosystem.

Therefore, the ITE Law can be considered partially effective. It provides legal instruments that can be applied to phishing and digital impersonation, especially where the conduct involves misleading information, unauthorized access, or manipulated electronic information. However, its effectiveness is limited by the absence of explicit phishing and digital impersonation provisions, the fragmented use of multiple articles, evidentiary challenges, and the difficulty of addressing early-stage deception before access or financial loss occurs. The law is useful as a normative basis, but it still requires clearer interpretation and stronger institutional support to respond effectively to the evolving methods of cybercrime.

3.2. Why Is the Regulation of Phishing and Digital Impersonation Urgent to Be Examined Under the Electronic Information and Transactions Law?

The urgency of examining phishing and digital impersonation under the ITE Law arises from the growing dependence of Indonesian society on digital platforms. Banking, e-commerce, public services, health services, education, and professional communication increasingly rely on electronic systems. This dependence creates a legal environment in which trust becomes a central element of digital security. When perpetrators impersonate banks, marketplaces, public agencies, delivery services, or customer support officers, they do not merely deceive individuals. They weaken institutional trust in the digital ecosystem. This makes phishing and digital impersonation legally significant because the harm extends beyond individual financial loss.

Digital impersonation is especially urgent because it exploits the symbolic authority of legitimate institutions. In conventional fraud, the perpetrator may personally persuade the victim. In phishing, the perpetrator can borrow the credibility of an institution through logos, profile names, domain similarities, business-account labels, automated replies, and imitation websites. Kusuma (2021) demonstrates this pattern in fake customer care accounts that targeted banking customers through social media. The legal problem is that victims may act reasonably in trusting an account that appears visually similar to an official channel. Therefore, the law must be able to distinguish ordinary online deception from structured identity misuse that manipulates digital trust.

The second urgency relates to the speed and scale of phishing. Unlike conventional fraud, phishing can be replicated rapidly through mass messages, social media replies, fake links, or automated bots. A single phishing template may be used against many victims with minimal cost. This creates a mismatch between the traditional case-by-case model of criminal enforcement and the technical reality of mass digital deception. Yulianto (2021) argues that Indonesia's cybersecurity policy still faces challenges because legal and institutional arrangements remain general, sectoral, and not fully integrated. This observation is relevant because phishing cases often involve multiple sectors, such as banking, telecommunications, platform governance, police investigation, and consumer protection. Without coordinated regulation, enforcement may become slow and fragmented.

The third urgency concerns victim protection. Phishing victims often experience not only financial loss, but also loss of personal data, account takeover,

reputational harm, psychological distress, and uncertainty about liability. Tantimin (2021) explains that online fraud has become easier because digital transactions allow offenders to exploit distance, anonymity, and limited verification. In phishing cases, victims may be blamed for voluntarily submitting OTP codes or credentials, even though their consent was obtained through deception. This raises a normative issue: whether existing legal protection is sufficiently victim-oriented. If the law focuses only on punishing perpetrators after loss occurs, it may fail to provide preventive protection for consumers who are exposed to sophisticated impersonation schemes.

The fourth urgency lies in legal certainty. The absence of an explicit phishing offense creates uncertainty for law enforcement officers, prosecutors, judges, victims, and digital service providers. Gulo et al. (2020) show that phishing can be linked to several ITE Law provisions, but this multiplicity also creates ambiguity. One case may be treated as manipulation of electronic information, another as false information causing consumer loss, and another as unauthorized access. While flexibility can be useful, excessive reliance on broad provisions may reduce predictability. A clear legal framework is needed so that perpetrators understand what conduct is prohibited, victims understand their legal position, and institutions understand their preventive obligations.

The fifth urgency concerns the relationship between cybercrime regulation and data protection. Phishing is often a data-driven crime. The immediate target may be credentials, identification numbers, banking information, or personal data. Once obtained, such data may be used for account takeover, identity fraud, social engineering, or further financial crimes. Although the ITE Law addresses electronic

information and system misuse, its focus is not exclusively personal data protection. This creates a gap because phishing does not always produce immediate financial loss, but it may produce serious data compromise. The legal response should therefore recognize that data theft and identity misuse are not merely preliminary acts, but central harms in phishing schemes.

The sixth urgency relates to institutional responsibility. Many phishing schemes exploit the gap between official and unofficial communication channels. Fake customer service accounts can appear because users complain publicly on social media, and perpetrators respond faster than official institutions. This shows that legal regulation should not only criminalize perpetrators, but also encourage institutions and electronic system providers to strengthen verification, public education, reporting channels, takedown mechanisms, and consumer warning systems. Mahira et al. (2020) emphasize that cyberattack prevention requires a multistakeholder and shared-responsibility approach. This perspective is important because phishing and digital impersonation involve users, digital platforms, financial institutions, telecommunications providers, regulators, and law enforcement agencies. If each actor works separately, the response will remain fragmented and reactive.

The need for institutional coordination is also reflected in Indonesia's cybersecurity governance development. Mulyadi and Rahayu (2018) explain that the establishment of the National Cyber and Crypto Agency, or BSSN, reflects the state's effort to strengthen national cybersecurity coordination. This institutional development is relevant to phishing and digital impersonation because both offenses

require rapid reporting, technical investigation, platform cooperation, and public education. Criminal provisions alone cannot remove fake accounts, secure compromised systems, or prevent repeated impersonation patterns. Therefore, the urgency of regulation also lies in connecting criminal law with cybersecurity institutions and operational response mechanisms.

The seventh urgency concerns the evolution of cybercrime methods. Phishing is not static. It can move from e-mail messages to social media replies, fake call centers, QR code fraud, mobile applications, imitation websites, and account-takeover schemes. Putra (2021) emphasizes that phishing operates through changing methods that combine technological manipulation and deception. This dynamic character requires legal interpretation that is flexible enough to cover new forms, but precise enough to avoid uncertainty. The current ITE Law provides broad provisions, yet broadness alone is not the same as effectiveness. A law may be broad enough to apply after harm occurs, but still insufficiently detailed to guide prevention, investigation, and institutional compliance.

For these reasons, the regulation of phishing and digital impersonation is urgent because it sits at the intersection of criminal law, consumer protection, personal data security, electronic evidence, cybersecurity governance, and digital trust. The ITE Law already provides a foundation, but its provisions remain dispersed across different legal categories. The normative challenge is to strengthen the law's clarity without losing flexibility. This can be done by developing more specific interpretive guidelines, improving coordination among cybercrime investigators and sectoral regulators, clarifying the legal meaning of digital

impersonation, and recognizing phishing as a distinct cybercrime pattern. Such strengthening would not only improve enforcement, but also enhance preventive protection for users and institutions operating in Indonesia's digital environment.

4. Conclusion

This study concludes that the Electronic Information and Transactions Law has provided an important legal basis for regulating phishing and digital impersonation in Indonesia, but its effectiveness remains partial. Several provisions in the ITE Law can be used to address different elements of phishing-related conduct. Article 28 paragraph (1) may apply when perpetrators distribute false or misleading electronic information that causes consumer loss. Article 30 may apply when stolen credentials are used to access an electronic system without authorization. Article 35 may apply when perpetrators create or manipulate electronic information, accounts, websites, or digital documents to make them appear authentic. These provisions show that the ITE Law is not irrelevant to phishing and digital impersonation. However, the law does not yet provide a specific formulation of phishing or digital impersonation as independent cyber offenses.

The main limitation of the ITE Law lies in its broad and fragmented structure. Phishing is often committed through several interconnected stages, including identity imitation, deceptive communication, credential collection, unauthorized access, and financial exploitation. Because the law does not expressly regulate phishing as a distinct offense, law enforcement must classify the conduct through separate provisions depending on which element can be proven. This may create

uncertainty in investigation, prosecution, and judicial interpretation. The problem becomes more complex when the loss suffered by victims is not immediately financial, but involves personal data exposure, account takeover, or misuse of digital identity. Therefore, the effectiveness of the ITE Law depends not only on the existence of criminal provisions, but also on the clarity, consistency, and adaptability of their application.

The urgency of regulating phishing and digital impersonation also lies in their broader implications for consumer protection, data security, cybersecurity governance, and public trust in digital services. These offenses exploit the credibility of legitimate institutions and can be rapidly replicated across social media, messaging platforms, e-mail, websites, and financial service channels. As a result, phishing cannot be understood merely as ordinary fraud committed through digital tools. It is a cybercrime pattern that combines deception, impersonation, unauthorized data acquisition, and institutional trust manipulation. A purely reactive legal approach is insufficient because victims may suffer harm before enforcement mechanisms can respond.

Accordingly, Indonesia needs to strengthen the regulatory framework by clarifying the legal meaning of phishing and digital impersonation, developing interpretive guidelines for relevant ITE Law provisions, and improving coordination between law enforcement agencies, cybersecurity institutions, financial service providers, digital platforms, and consumers. The law should remain flexible enough to respond to evolving cybercrime methods, but precise enough to provide legal certainty. Strengthening the framework would improve enforcement, enhance

preventive protection, and support a safer digital environment for Indonesia's growing electronic transaction ecosystem.

References

Adhi, M. I. P., & Soponyono, E. (2021). Crime combating policy of carding in Indonesia in the political perspective of criminal law. *Law Reform, 17*(2), 135–144.

Alfian, M. (2017). Penguatan hukum cyber crime di Indonesia dalam perspektif peraturan perundang-undangan. *Kosmik Hukum, 17*(2).

Aulianisa, S. S., & Indirwan, I. (2020). Critical review of the urgency of strengthening the implementation of cyber security and resilience in Indonesia. *Lex Scientia Law Review, 4*(1), 33–48.

Fuad, A. N. (2021). Misuse of credit cards or carding in Indonesia: How is the law enforced? *Law Research Review Quarterly, 7*(1), 83–96.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2020). Cyber crime dalam bentuk phising berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law, 1*(2), 68–81.

Koto, I. (2021). Cyber crime according to the ITE Law. *International Journal Reglement & Society, 2*(2), 103–110.

Kusuma, H. (2021, March 14). Hati-hati! Banyak akun customer care palsu gentayangan di medsos. *detikFinance*. Retrieved Jan 1, 2022 from https://finance.detik.com/berita-ekonomi-bisnis/d-5492485/hati-hati-banyak-akun-customer-care-palsu-gentayangan-di-medsos

Mahira, D. F., Rohmahwatin, D. S., & Suciningtyas, N. D. (2020). Strengthening multistakeholder integrated through shared responsibility in the face of cyber attacks threat. *Lex Scientia Law Review, 4*(1), 63–74.

Mulyadi, M., & Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment National Cyber and Crypto Agency (BSSN). In *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (pp. 37–42). IEEE.

Putra, V. F. (2021). Modus operandi tindak pidana phising menurut UU ITE. *Jurist-Diction, 4*(6), 2525–2548.

Tantimin, T. (2021). Legal liability of minors as perpetrators of online buying and selling fraud in Indonesia. *Law Reform, 17*(2), 145–156.

Tanujaya, A. (2021, February 17). Awas! Jangan sampai tertipu call center BCA palsu. *detikInet*. Retrieved March 3, 2022 from https://inet.detik.com/security/d-5377452/awas-jangan-sampai-tertipu-call-center-bca-palsu

Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. *Law Research Review Quarterly, 7*(1), 69–82.