Jurnal Bina Mulia Hukum

Contents lists available at Sinta 2

JURNAL BINA MULIA HUKUM

Journal homepage: https://jurnal.unpad.ac.id/jbmh

Analysis of The Ite Law and Criminal Acts of Carding and Phishing in Indonesia

Didit Darmawan[a*], **Rommy Hardyansah**[b], **Al-Araf Assadallah Marzuki**[c]

[a, b] *Universitas Sunan Giri Surabaya, Indonesia.*
[c] *Badan Riset Inovasi Nasional, Indonesia.*
[*] *Corresponding Author: dr.diditdarmawan@gmail.com*

ARTICLE INFO

Volume 10, Number 1, 2025
(1-17)
DOI: https://doi.org/10.23920/jbmh.v10i1.1527
P-ISSN: 2528-7273
E-ISSN: 2540-9034

Article History:
Submitted: 23/11/2023
Revised: 13/07/2025
Accepted: 29/10/2025
Published: 30/10/2025

Keywords: carding; cybercrime; phishing.

ABSTRACT

The advancement of information and communication technology in Indonesia has increased cybercrimes such as carding and phishing. Although the Electronic Information and Transactions (ITE) Law No. 19 of 2016 regulates sanctions, it lacks specificity in addressing the evolving methods of cybercrime, making law enforcement and public protection more difficult. This research evaluates the effectiveness of the ITE Law against carding and phishing, analyzes its implementation, and offers recommendations to make adaptive regulations to new cybercrime methods. It offers a critical analysis of legal and implementation gaps related to carding and phishing, emphasizing the urgency of law reform and the integration of preventive strategies. This study uses a mixed-method approach, combining legal document analysis and empirical surveys to assess the effectiveness of the ITE Law and identify challenges in tackling carding and phishing crimes. The results show that while the ITE Law offers a legal foundation, it lacks sufficient detail to address new cybercrime methods. There is a need for more specific regulations, stronger inter-agency cooperation, improved digital literacy, and stricter sanctions. Preventive efforts such as education, stronger security, and collaboration are essential to reduce risks and close legal gaps.

INTRODUCTION

Currently, the rapid advancement of information and communication technology is observable worldwide, including in Indonesia, as demonstrated by the increasing utilization of computers, laptops, mobile devices, and internet connectivity among the general population.[1] This advancement has facilitated communication and simplified tasks that were previously complex, affecting nearly every aspect of human life.[2] In globalization era, the role of information and communication technology becomes crucial as it connects the world without geographical, time, and spatial boundaries, ultimately enhancing productivity and efficiency.[3] This role began with the development

[1] Daryanto Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Budaya," *Jurnal Simbolika Research and Learning in Communication Study* 4, no. 1 (2018): 62–72.
[2] Muhammad Sukron Djazilan and Didit Darmawan, "The Effect of Religiosity and Technology Support on Trust in Sharia Banking in Surabaya," *Journal of Science, Technology and Society* 2, no. 2 (2021): 7–18.
[3] Charles Kenny, "Information and Communication Technologies for Direct Poverty Alleviation: Costs and Benefits," *Development Policy Review* 20, no. 2 (2002): 141–157, https://doi.org/10.1111/1467-7679.00162; Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Budaya."

of communication and data technology that facilitated human interaction.[4] In facing this development, all parties must optimize the use of technology. The process of globalization began simultaneously with the development of communication and information technology.[5] Life dependent on communication and technology must be utilized to its fullest potential.[6]

Business transactions today no longer require physical meetings but can be conducted through computers and telecommunications.[7] This marks the beginning of the online business era. However, this era is followed by cybercrimes as a negative effect of technological progress, including carding and phishing. Some cybercrimes, such as increasingly sophisticated ransomware attacks, target various entities, including large companies, government institutions, and critical infrastructure.[8] Cybercriminals often demand ransom payments in crypto currency to decrypt encrypted data. They also target Internet of Things (IoT) devices, such as smart home systems, surveillance cameras, and medical equipment, as more of these devices connect to the internet. Meanwhile, carding refers to the unauthorized use of someone's credit card, either by physically duplicating the card or by using hacking techniques to make illegal purchases or withdraw money from the victim's account.[9] In Indonesia, carding cases have been rapidly increasing, with around 20% of total credit card transactions over the internet categorized as cyber fraud activities.

In addition to carding, crimes executed by individuals engaging in cracking or being crackers include phishing. Phishing is an attempt to obtain personal information by directing individuals to fake websites with the intent of illegal gain.[10] Phishing is a form of deception aimed at stealing personal and confidential data while posing as a trusted source or legitimate organization, often through electronic communication.[11] Phishing attacks have become increasingly sophisticated. Attackers are becoming more skilled at designing deceptive phishing campaigns that are difficult to detect. They often employ advanced social engineering techniques to manipulate their victims, a consequence of their growing skills and resources. With the growth of online shopping behavior in Indonesia, there is an increased potential for phishing attacks. In 2021, over 50% of Indonesia's population engaged in online shopping, a number that continues to rise with the digital

[4] Muhammad Khairi and Didit Darmawan, "Blockchain Enforcement in Employee Data Management to Increase Transparency and Security," *International Journal of Service Science, Management, Engineering, and Technology* 7, no. 2 (2025): 1–5.
[5] Mukti Kemarauwana and Didit Darmawan, "Perceived Ease of Use Contribution to Behavioral Intention in Digital Payment," *Journal of Science, Technology and Society* 1, no. 1 (2020): 1–4.
[6] Shan L. Pan and Dorothy E. Leidner, "Bridging Communities of Practice with Information Technology in Pursuit of Global Knowledge Sharing," *The Journal of Strategic Information Systems* 12, no. 1 (2003): 71–88, https://doi.org/10.1016/S0963-8687(02)00023-9; Tugrul U. Daim et al., "Exploring the Communication Breakdown in Global Virtual Teams," *International Journal of Project Management* 30, no. 2 (2012): 199–212, https://doi.org/10.1016/j.ijproman.2011.06.004; Didit Darmawan and E Retnowati, "Peranan Kepercayaan dan Keamanan terhadap Minat Belanja di Tokopedia," *Jurnal Ekonomi Dan Bisnis* 3, no. 1 (2013): 1–6.
[7] R B Harris and D Paradice, "An Investigation of the Computer-Mediated Communication of Emotions," *Journal of Applied Sciences Research* 3, no. 12 (2007): 2081–2090.
[8] W Wahyudi et al., "Big Data and New Things in Social Life," *Studi Ilmu Sosial Indonesia* 1, no. 1 (2021): 1–12.
[9] Nur Muchammad Ivan Firmansyah and Luki Nurfanto, "Pertanggung Jawaban Pidana Carding terhadap Pengguna Kartu Kredit," *Mimbar Keadilan* 14, no. 2 (2021): 206–217.
[10] Rika Butler, "A Framework of Anti-Phishing Measures Aimed at Protecting the Online Consumer's Identity," *The Electronic Library* 25, no. 5 (2007): 517–533.
[11] John Thompson Okpa et al., "Rising Trend of Phishing Attacks on Corporate Organisations in Cross River State, Nigeria," *International Journal of Cyber Criminology* 14, no. 2 (2020): 460–478.

infrastructure's development in the country.[12] The proliferation of e-commerce platforms and online financial services in Indonesia provides more opportunities for attackers to attempt data breaches of personal and financial information.[13] This leads them to develop new techniques in their phishing practices, including the use of fake messages, phishing websites, and imitation of well-known brands. With the increasing sophistication of phishing attacks, it is crucial for users to enhance their online awareness and security.

Phishing often targets online banking users to steal personal information such as IDs and passwords, but it can also occur through social media, email or SMS. Phishing is done by sending deceptive messages, claiming, for example, that the user has won a lottery prize or needs help with a problem that does not exist. Phishing has become an increasingly serious problem, with phishing scams accounting for 42% of all fraud modes in a report published by the Anti-Phishing Working Group (APWG). Statistics show a significant increase in phishing attacks, reaching approximately 263,538 cases of attacks during the first quarter of 2018, marking a 46% increase compared to the previous quarter.[14] In Indonesia, the last five years have seen a drastic increase in phishing attacks. By 2023, phishing attack attempts jumped more than 40 percent to reach approximately 709 million phishing attack attempts.[15]

Legal regulations regarding acts such as phishing in Indonesia are essential to provide a clear framework for addressing cybercrime. Law No. 19/2016 on the Amendment to Law No. 11/2008 on Electronic Information and Transactions (ITE Law) is a significant first step in addressing cybersecurity issues in Indonesia. Even though, Indonesian law already regulates acts like phishing, but there are questions about whether these rules are enough or if other laws, such as the Criminal Code, should also be considered. Law No. 1/2023 of the Criminal Code has been introduced to help address cybercrime more effectively. Although the Criminal Code was not originally designed specifically for cybercrime cases, the revised Criminal Code has been adjusted to accommodate new crimes that emerge along with technological advances. ITE Law establishes regulations on phishing and other cybercrimes that harm others in the digital realm in electronic transactions, in line with the rapid development of information technology. Law No. 1/2023 has also specialized in the Section on Crimes against Informatics and Electronics from Article 332 to Article 335.

Advancements in online commerce have also brought about changes in the law.[16] ITE Law regulate legal aspects related to carding and phishing, including illegal access to others' electronic information, illegal electronic surveillance, destruction and illegal transfer of confidential electronic

[12] Arif Rachman Putra et al., "Analysis of the Influence of Privacy, Security and Ease of Use on Intention to Shopping through the Marketplace," *Journal of Marketing and Business Research* 3, no. 1 (2023): 35–48.
[13] Ella Anastasya Sinambela and Didit Darmawan, "Advantages and Disadvantages of Using Electronic Money as a Substitute for Cash," *Journal of Social Science Studies* 2, no. 2 (2022): 56–61.
[14] Ayesha Warda and Jhumur Samaddar, "A Primary Study on User Perception of Phishing in Banking Sector," *SJCC Management Research Review*, August 13, 2022, 59–79, https://doi.org/10.35737/sjccmrr/v12/i1/2022/155.
[15] CNN Indonesia, "Serangan Phising Meningkat 40 Persen Sepanjang 2023, Cek Targetnya," CNN Indonesia, 2024, https://www.cnnindonesia.com/teknologi/20240313142500-192-1073789/serangan-phishing-meningkat-40-persen-sepanjang-2023-cek-targetnya.
[16] N Nurhadi et al., "Analysis of Value Added Tax Application on Electronic Commerce Transaction in Digital Economy System in Indonesia," *Journal of Social Science Studies* 3, no. 2 (2023): 83–88.

information, distribution or provision of tools for crimes, and manipulation of illegal electronic information. This law applies both within and outside Indonesia's jurisdiction, if it has legal implications in Indonesia and harms Indonesia's interests. In addition ITE Law also reaffirms the legal framework related to cybercrimes, including phishing and carding, in Indonesia. Furthermore, other relevant regulations or amendments can continue to be applied or proposed to address the evolving landscape of cybercrimes. There may also be additional regulations or laws developed to accommodate technological advancements and the latest online behavioral trends. Therefore, it is essential to stay updated on the latest legal developments and their implementation concerning cybersecurity in Indonesia.

Governments in various countries have adopted policies and programs to address cybersecurity threats. In Indonesia, several steps and initiatives have been taken, such as updating regulations regarding the use of information technology and electronic transactions. Despite undergoing several revisions and amendments, ITE Law still shows a number of weaknesses that affect its effectiveness in dealing with cybercrimes. The revision of ITE Law and the second amendment through Law No. 1/2024 aim to expand the scope of cybersecurity, but in practice, some articles are not specific enough and sometimes overlap with provisions in the Criminal Code. This causes difficulties in law enforcement, especially in addressing new modes such as carding and phishing that continue to evolve with digital technology.[17] In addition, some of the rules in the ITE Law are still considered ineffective due to duplication with articles of the Criminal Code, thus requiring in-depth studies to harmonize and clarify the scope of applicable laws so as not to cause multiple interpretations and inconsistencies in handling cyber cases.[18]

With the enactment of Law No. 1/2023 which regulates Article 332 to Article 335 concerning special criminal offenses, including cybercrime, it is expected that legal gaps previously not covered in the ITE Law will be addressed. However, this adjustment also requires strengthening the synergy between regulations so that the handling of carding and phishing cases can be integrated effectively. Since these crimes are very dynamic and involve sophisticated technological methods, the existing law must be able to adapt and provide clear legal protection. Therefore, focused studies are needed to evaluate the effectiveness of both the ITE Law and the revised Criminal Code in addressing cybercrime, ensuring optimal legal protection and deterrence for offenders.[19]

Moreover, the government has collaborated with law enforcement agencies and relevant institutions to enhance supervision and enforcement against cybercrimes. This includes investigating, arresting, and prosecuting offenders. Special teams and agencies have also been established to manage cybersecurity, detect and respond to cyber-attacks, secure critical infrastructure, and

[17] Adi Putra Manggala et al., "Legal Review of the Implementation of Electronic Contracts and Protection of Parties in Digital Transactions in Indonesia," *International Journal of Service Science, Management, Engineering, and Technology* 8, no. 1 (2025): 1–8.
[18] Rahma Agri Firdaus, "Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum Di Indonesia," *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2025): 79–104, https://doi.org/10.14421/cf582q68.
[19] M Irfan and Dharma S Negara, "The Effectiveness of Consumer Protection Arrangements in E-Commerce Transactions on the Shopee Marketplace Platform in Indonesia," *Journal of Social Science Studies* 3, no. 2 (2023): 115–120.

provide policy recommendations. In certain cases, international cooperation is also involved, with Indonesia participating in information exchange and coordination with other countries to addressing cross-border cybercrime effectively.

In essence, the increasing integration of digital technology into daily transaction has changed how legal relationships work between individuals and institutions. Legally, these transactions are still governed by existing laws, despite the shift from physical to digital mediums. Therefore, this study aims to analyze how advancement in information and communication technology has impacted society in Global, with a focus on negative consequences such as the rise in carding and phishing cases. Furthermore, this study seeks to examine government policies and programs related to cybersecurity and to propose recommendations to enhance the effectiveness of implementation of the ITE Law.

METHODS

This research uses a mixed method that combines normative and empirical approaches to provide a comprehensive analysis of the criminal acts of carding and phishing in online transactions. The normative approach is used to understand, analyze, and provide legal views based on existing literature and regulations, particularly the ITE Law and its revisions. It is used to conduct an in-depth study of carding and phishing crimes that occur in online buying and selling transactions and provide constructive ideas for prevention and strengthening the implementation of the ITE Law. The main sources in this analysis are legal documents and legal literature that discuss aspects of illegal access, carding, phishing, electronic fraud, and applicable sanctions.

Practically, normative approach is combined with empirical element in form of case study analysis to obtain a real picture of the effectiveness of the implementation of the ITE Law and the challenges faced in law enforcement against carding and phishing. The results will be used to develop a comprehensive legal outlook as well as constructive recommendations in addressing the problems of carding and phishing, both in terms of regulation and public policy. It is hoped that this study can strengthen the legal framework governing carding and phishing in the ITE Law and make a real contribution to the protection and enforcement of law in the current era of advanced technology.

DISCUSSION

In addressing electronic transaction crimes such as carding and phishing, it is important to understand that the law exists to protect the public and impose sanctions on perpetrators. The legal regulations concerning electronic transaction crimes can be explained as follows:

Trends and Changes in Global Phishing Attack Strategies

Data from the Anti-Phishing Working Group (APWG) shows a global phishing attack trend with a peak in the first quarter of 2023 and a shift in attack targets in the first quarter of 2025[20] as shown in the following table 1 below:

Table 1.
Trends in quarterly phishing attacks numbers based on APWG data from 2023 to the first quarter of 2025.

Quarter	Year	Number of Phishing Attacks
Q1	2023	1,624,144 (record high)
Q2	2023	1,286,208
Q3	2023	999,956
Q4	2023	1,077,501
Q1	2024	963,994
Q2	2024	877,536
Q3	2024	932,923
Q4	2024	989,123
Q1	2025	Data not directly available, but SAAS/Webmail accounts for 17.6% of total attacks, with an increase in attacks targeting payment and banking sectors (30.9%)

Source : APWG

Based on the table 1, the following observations can be made:

a. The highest peak occurred in Q1 2023 with over 1.6 million attacks. Following this, there was a significant decline until Q3 2023, reaching approximately 1 million attacks, representing a decrease of about 38% from Q1 to Q3 2023.
b. From Q4 2023 to Q4 2024, fluctuations were observed with a slight downward trend followed by a rebound in the second half of 2024, with the number of attacks ranging between 877,536 and 989,123 per quarter.
c. The monthly number of attacks during this period ranged from 290,000 to 370,000, indicating a stabilization in the monthly attack rate after the sharp decline earlier in 2023.
d. The increase in attacks targeting the online payment and banking sectors in Q1 2025 indicates a shift in phishing actors' focus toward sectors that are more vulnerable and financially valuable.

Regarding the distribution of attacks by sector in Q1 2025:

a. SAAS/Webmail accounted for 17.6% of all phishing attacks, down from 23.3% in Q4 2024.
b. Online Payment and Financial (Banking) sectors accounted for 30.9% of all attacks, showing an increase in attacks in this sector from Q4 2024 to Q1 2025.

[20] Anti-Phishing Working Group (APWG), *Phishing Activity Trends Report*, First Quarter 2025 (2025), https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf.

The decline in phishing attacks targeting the SAAS/Webmail sector, along the rise in attacks on financial and payment sectors, indicates that phishing actors have shifted their focus toward areas offering greater economic gain. This change demonstrates a more strategic and profit driven selection of targets.

Meanwhile, the decline in reported phishing cases in 2024, particularly in the second quarter, appears linked to technical challenges, mainly restrictions from email services providers that limit users' ability to report phishing attempts. Despite fewer reported cases, the number of unique phishing campaigns increased significantly by 64% in the fourth quarter of 2024. This indicates that cybercriminals are diversifying their methods to evade advanced security systems and detection filters, demonstrating their ongoing adaptability to tighter cybersecurity measures. In summary, phishing attacks dropped by about 38.4% from 1,624,144 in Q1 2023 to 999,956 in Q3 2023. However, they rose again by around 12.7% from Q2 2024 (877,536) to Q4 2024 (989,123). The share of SAAS/Webmail attacks declined from 23.3% in Q4 2024 to 17.6% in Q1 2025, while attacks on payment and banking sectors increased to 30.9%, confirming this shift in focus.

Overall, phishing attacks peaked in early 2023 before stabilizing at around 900,000 to 1,000,000 per quarter throughout 2024. Although the total number of attacks leveled off, their nature evolved: cybercriminals increasingly targeted financial sectors and expanded the variety of attack methods. These developments highlight their continuous adaptation to exploit vulnerable yet high-value targets. Finally, it is important to interpret reported data cautiously. Technical limitations in phishing reporting systems may have affected the completeness of recorded figures, meaning that the actual number of incidents could be higher than reported.

Anticipating the Threat of Carding Crimes in the Age of Advanced Technology

According to Article 30, Paragraphs (1), (2), and (3), Article 31, Paragraphs (1) and (2), Article 32, Paragraphs (1) and (2), Article 34, Article 35, Article 36, and Article 40, Paragraphs (1) and (2) of ITE Law, especially in relation to carding crimes, it can be concluded that existing laws still rely on old regulations. Therefore, more detailed and specific rules addressing carding are necessary. In addition, the security of both software and hardware systems must be optimized to ensure high quality and reliability, and clear guidelines should be established for decision-makers handling computer-related crimes.

Current regulations may not fully accommodate the emerging issues related to technological advancement and cybercrime.[21] Hence, more specific and detailed regulations concerning carding are needed. In addition to regulatory efforts, the government should adopt both punitive and non-punitive measures. Punitive efforts involve stricter law enforcement against perpetrators of computer crimes, while non-punitive measures focus on public education, awareness campaign, and training to strengthen online transaction security. Furthermore, the role of specialized institutions should be enhanced to help minimize and prevent online transaction crimes. These strategic steps,

[21] Erik P Bucy et al., "Performing Populism: Trump's Transgressive Debate Style and the Dynamics of Twitter Response," *New Media & Society* 22, no. 4 (2020): 634–58, https://doi.org/10.1177/1461444819893984.

including developing targeted regulations, improving enforcement, and empowering relevant institutions, are essential to ensure that the law keeps ace with technological developments and effectively mitigates cybercrime risks. To initiate these actions, the following concrete steps can be taken:

a. Stakeholder Collaboration: Organize forums and meetings involving the government, legal experts, academics, technology industry, and cyber security agencies to discuss regulatory needs and draft new policies. In these forums, stakeholders can exchange insights on cyber security issues and the latest technological developments, ensuring that resulting regulations are comprehensive, relevant, and balanced in protecting all parties in the digital ecosystem.
b. Regulation Drafting: Establish a specialized team of legal and technology experts, and community representatives, to draft detailed regulations on carding. This team should conduct thorough research on legal and technical aspects of carding and consult relevant stakeholders to ensure that the drafted regulations genuinely meet the needs and demands of all parties involved.
c. Strict Law Enforcement: Enhance the capacity of law enforcement agencies to take firm action against computer crime perpetrators, including carding, through effective investigation and prosecution. Moreover, strengthening collaboration with cybersecurity agencies and other relevant institutions to ensure fair and consistent enforcement of new regulations. Strengthening law enforcement is expected to create a deterrent effect and reduce the prevalence of carding crimes in society.
d. Public Education and Awareness Campaigns: Conduct education and awareness campaigns through mass media and online platforms to inform the public about the risks and impacts of computer crimes and ways to protect themselves. Collaboration with technology experts, legal professionals, and cyber security agencies is essential to develop clear and accessible educational materials. These campaigns aim to increase public awareness of cybercrime risks, including carding, and provide them with the knowledge and skills needed for safe online transactions.[22]
e. Online Security Training Programs: Organize training sessions and workshops for the public, especially active internet users and online shoppers, to improve their understanding of online security practices. These programs should involve cybersecurity and technology experts in developing practical and accessible training materials, supported by collaboration with online communities and educational platforms. The goal is to equip the public with the skills needed to protect themselves during online activities, thereby reducing the risk of cybercrimes such as carding.
f. Consultation with Technology Experts: Invite technology and cybersecurity experts to provide input on software and hardware security and assist in developing security guidelines. In these consultations, regular meetings with professionals from fields such as software, networking,

[22] Y. G Anugroh et al., "Consumer Protection and Responsibilities of E-Commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions," *Journal of Social Science Studies* 3, no. 2 (2023): 89–94.

and cybersecurity should be held to gather insights and best practices for securing digital infrastructure. Collaboration with research institutions and universities is also essential to ensure continuous innovation and updates in security measures. These consultations aim to help the technology industry implement effective protections aligned with the latest technological advancements.

g. Periodic Evaluation and Revision: Establish mechanisms for periodic evaluations of existing regulations to ensure their continued relevance amid technological advancements. This periodic evaluation process should involve legal and technology experts along with key stakeholders to review current laws, identify weaknesses or gaps, and provide recommendations for revisions or necessary changes. The goal is to ensure the regulations remain relevant and effective in dealing with new challenges and risks in the digital world.
h. Establishment of Oversight Institutions: Establish a specialized oversight body or strengthening existing institutions to monitor and supervise online transactions regulations and security standards. These institutions should have the authority to monitor both businesses and consumers, ensuring adherence to newly implemented rules. Collaboration with government bodies, law enforcement agencies, and civil organizations is essential to maintain security, transparency, and accountability in the online transaction environment.
i. International Collaboration: Collaborate with international institutions in terms of law enforcement related to computer crimes and electronic transaction. Such collaboration enables the exchange of information, experiences, and resources to enhance global law enforcement efforts. Through cross-border coordination, computer crimes involving perpetrators from various regions can be addressed more effectively. Moreover, harmonizing electronic transaction regulations can create a more organized and secure global legal framework.
j. Testing and Simulation: Perform testing and simulation of electronic security systems to identify potential vulnerabilities and ensure the effectiveness of implemented security strategies. These activities help identify and address potential vulnerabilities before fully deployed, ensuring systems are capable of responding to diverse cybersecurity threats. Through continuous testing, the overall security and reliability of digital systems can be strengthened against evolving risks.

These actions represent concrete steps to initiate the implementation of these ideas. By involving various stakeholders and considering regulatory, public education, and technological aspects, it is expected that these ideas can form a strong foundation for protecting the public from carding and similar cybercrimes. Through collaboration, the development of specific regulations, law enforcement, educational campaigns, online security training, and consultations with technology experts, a safer and more trustworthy legal and technological environment for electronic transactions can be achieved. As a result, public can use technology in confidence and secure, without worrying on the risks of computer crimes.

Since 2008, the Indonesian government has taken steps to combat cybercrime by implementing Law Number 11 of 2008 concerning Electronic Information and Transactions. While this was a significant initial step, the rapid evolution of technology and the complexity of computer crimes, including carding, indicate the need for further efforts. In the context of recent regulations, the Indonesian government has continuously worked to update and strengthen the legal framework related to cybercrime. The Government Regulation in the Lieu of Law No. 82 of 2012 concerning the Organization of Electronic Systems and Transactions was issued namely Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation places a stronger emphasis on security and data protection in electronic transactions. Moreover, Bank Indonesia issued Regulation Number 18/40/PBI/2016 concerning the Implementation of Payment Transactions. This regulation addresses the security and management of electronic payment transactions, an area vulnerable to computer crimes like carding. Furthermore, Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (P2SK) and Bank Indonesia Regulation No. 3 of 2023 on the Implementation of Payment Transactions (PKBI) further reinforce the regulatory framework, providing updated provisions to accommodate technological innovation and mitigate cyber risks in the financial sector. In the following years, the government has continued to evaluate and refine digital security-related regulations. With the issuance of new laws and regulations, the government aims to accommodate technological developments and counter increasingly complex cyber threats. Beside the regulatory aspects, education aspect plays a crucial role in fighting computer crimes. Training and education on digital security and online ethics need to be continuously improved and integrated into both formal and non-formal education systems. Through comprehensive efforts such as regulation revisions, education, and cross-sector cooperation, Indonesia can strengthen its defense against computer crimes, including carding, and build a safer and more trustworthy digital ecosystem for all members of society.

Anticipating the Threat of Phishing Crimes

The threat of phishing crimes has become a serious challenge in the age of advancing information technology, reflecting the evolution of cybercrime alongside digital progress.[23] To safeguard public security, comprehensive preventive measures and public education on phishing risks are imperative. Phishing attacks can inflict severe financial and reputational damage on individuals and institutions alike. Therefore, active collaboration among the government, the technology industry, and cybersecurity institutions is essential to strengthen defenses and create a safer, more reliable digital ecosystem. By increasing awareness of phishing risks and implementing effective security strategies, the public can better protect themselves and maintain safety in the ever-evolving digital era. To minimize risks and enhance information security, several proactive measures should be adopted. The following are key preventive actions that can be implemented:

[23] Ike Vayansky and Sathish Kumar, "Phishing – Challenges and Solutions," *Computer Fraud & Security* 2018, no. 1 (2018): 15–20, https://doi.org/10.1016/S1361-3723(18)30007-1.

a. Education and Training: Efforts in educating and training people regarding phishing tactics and techniques should be a priority. Users should be educated to identify common characteristics and behaviors of phishing attacks, such as suspicious emails and deceptive links. Education and training related to phishing tactics and techniques are fundamental and strategic. This education should be a top priority in mitigating the risks of phishing crimes. For example, users should be able to recognize suspicious emails and links specifically designed to deceive and manipulate personal information. Education and training should be systematically and comprehensively designed. This includes providing relevant educational materials, conducting phishing attack simulations, and equipping users with adequate technical knowledge to distinguish between official communication and phishing attempts. Additionally, there is a need to develop evaluation methods to ensure the understanding and skills acquired by users in dealing with phishing threats. Learning resources and platforms can be utilized to disseminate information related to phishing.[24] Through collaboration between the government, educational institutions, and the private sector, educational initiatives prioritizing phishing prevention can be established. This will help build the capacity and awareness of the public regarding this threat, ultimately enhancing the level of security and well-being in the evolving information technology era.
b. Be Cautious with Unfamiliar Emails and Messages: Users should avoid opening or clicking links in emails or messages from unknown or suspicious sources. It is recommended to always verify the authenticity of emails and messages before taking further action. Users can check the sender's address, language structure, and whether the requested information is reasonable within the context of the ongoing transaction or communication. Whenever there is a request for sensitive information, it is important to verify the authenticity and credibility of the request before providing the requested information. This reduces the risk of falling victim to phishing attacks.
c. Use Reliable Security Systems: The installation and regular updates of security software, including firewalls, antivirus, and antispyware, are crucial steps in protecting systems from phishing threats. Implementing reliable security systems is a crucial aspect of countering phishing threats. Regularly installing and updating security software such as firewalls, antivirus, and antispyware is a proactive step to protect systems from phishing attacks. With this action, the risk of information leaks and vulnerability to phishing practices can be significantly minimized.
d. Check Website Addresses: Before entering sensitive information or login credentials, make sure that the website's address is legitimate and valid. Ensure that the URL matches the intended website. Checking website addresses before entering sensitive information or login credentials is a very important step. Make sure that the website address you are using is legitimate, and valid, and confirm that the URL matches the intended site. This helps prevent

[24] M Munir et al., "Implementation of Consumer Protection Principles in Overcoming the Problem of Ticket Sales by Scalpers through E-Commerce Platforms," *Journal of Social Science Studies* 3, no. 1 (2023): 145–52.

falling into phishing traps where users are directed to fake websites designed solely to steal personal information or logins. By being vigilant about the validity of websites, the risk of falling victim to phishing can be avoided.

e. Use Two-Factor Authentication: The use of two-factor authentication is an additional layer of highly effective security. This method requires additional verification beyond a password. Two-factor authentication is a highly effective security measure. This method requires additional verification beyond a password, such as a verification code sent via text message or an authenticator app. By implementing two-factor authentication, the risk of unauthorized access or identity theft through phishing methods can be significantly reduced.
f. Investigate Email Attachments: Avoid opening attachments from unknown or suspicious emails. Attachments may contain malware or viruses that can harm the system. Before opening an attachment, ensure that the sender is trustworthy and the purpose of sending the attachment is credible. Also, use security software to scan attachments and ensure there are no security threats before opening them. This step is crucial in reducing the risk of potential phishing threats.
g. Use Email Filters: Enable and configure spam and phishing filters in email settings. This step helps identify and separate suspicious emails. Spam and phishing filters can sort emails based on specific characteristics often associated with phishing attempts. By enabling this feature, users can reduce the likelihood of receiving or opening phishing emails.
h. Report Phishing Attacks to Email Providers or Relevant Institutions: Reporting phishing attacks is a key step in combating this criminal activity. By informing email providers or relevant institutions, information about the attack can be conveyed to the authorities for further investigation. Reporting phishing attacks is a crucial step in fighting this criminal activity. By informing email providers or relevant institutions, information about the attack can be conveyed to the authorities for further investigation. This will also help in taking more effective preventive actions in the future.
i. Monitor Financial Activities: Regularly checking and monitoring financial activities is a recommended step to detect suspicious or unauthorized transactions. Efforts to regularly monitor financial activities are a proactive measure that can help users identify potential phishing activities or unauthorized financial transactions. By checking accounts and transactions regularly, users can take immediate action if anything suspicious or unusual is detected in their financial activities.[25]

With the implementation of these preventive measures, it is expected that the risk and damage from phishing attacks can be reduced. In a constantly evolving world of information technology, information security and protection are essential and cannot be ignored. The ITE Law provides a legal foundation for addressing cybercrimes, including phishing which specifically regulated under Article 35 in conjunction with Article 51(1). These provisions stipulate that any individual who intentionally

[25] Oriento et al., "Risks and Legal Protection in Non-Cash Financial Transactions through E-Wallets," *Journal of Social Science Studies* 3, no. 1 (2023): 109–114.

and unlawfully manipulates, accesses, or creates electronic information or documents with the intention of making it appear authentic may be subject to criminal sanctions. This regulation directly applies to phishing actors who steal victims' personal information with particular aims, such as identity theft or financial fraud.[26]

A juridical analysis of the ITE Law affirms that national law has been responsive to the evolution of digital crime by accommodating legal protection for victims of phishing. In addition to imprisonment, perpetrators may be subject to fines designed both to deter future offenses and to safeguard the public. Nevertheless, the implementation of the ITE Law faces several challenges, including uneven levels of digital literacy in society and the continuously evolving methods of phishing. Therefore, alongside legal enforcement, preventive measures through public education and the strengthening of cybersecurity infrastructure are essential for ensuring that legal protection for victims remains effective and adaptive.

The legal framework related to cybercrimes in the form of phishing is also supported by Article 378 of the Indonesian Penal Code (KUHP), which regulates fraud. This article stipulates that anyone with the intent to gain profit illegally, whether for themselves or others, through the use of a false identity or false reputation, deception tactics, or a series of lies, induces others to hand over property or give loans, or erase debts, may be subject to imprisonment for up to four years as a penalty. In line with legal reform, Law No. 1/2023 on the Criminal Code, which came into force three years after its enactment (i.e. 2026), strengthens the regulation of criminal offenses including in the context of cybercrime. The article provides a strong legal basis for the prosecution of fraud crimes including phishing, with a maximum imprisonment of 4 years (Article 492 of Law No. 1/2023). However, cyber fraud still refers to Article 378 of KUHP as its main legal basis. The ITE Law complements this framework by providing additional provisions for fraud committed through information technology, though the core sanctions remain derived from the Penal Code.

Article 378 of KUHP that regulates fraud does not explicitly accommodate cybercrimes, particularly in the form of phishing. This limitation arises because the provision was formulated in an era when information technology and electronic transactions had not yet become significant phenomena. Consequently, the article lacks definitions of key elements such as technological manipulation and electronic deception used to obtain sensitive information. In phishing cases, these aspects are central to the offense, yet they are not clearly addressed within the current legal framework. This omission creates potential legal gaps that cybercriminals could exploit to evade accountability. To address this inconsistency, a review and refinement of the existing law is necessary. This would provide a stronger legal basis for dealing with cybercrimes, adapting to technological developments, and ensuring effective enforcement against cybercrimes for the safety and protection of the public in this complex digital world. The enactment of the ITE Law has gained a more specific and up-to-date legal foundation that aligns with current technological developments. This is mainly due to the principle of *Lex Specialis Derogat Legi Generali*, which means that legal

[26] Erfan Mukhlas Ali et al., "Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia," *International Journal of Service Science, Management, Engineering, and Technology* 6, no. 3 (2024): 27–38.

provisions with specific characteristics will take precedence in case of a conflict with general legal rules. Therefore, the ITE Law is an adequate and relevant legal instrument to address the phenomenon of phishing in the context of rapid information technology developments.

In the context of law enforcement against cybercrimes, including phishing, the Indonesian legal system sets strict and proportionate sanctions. The range of imprisonment penalties can vary from 6 to 12 years, along with fines that can amount to a significant sum, even reaching billions of rupiahs. The severity of the penalty is influenced by the seriousness of the offense and the extent of the losses caused by the phishing act. The Indonesian legal system adopts the principle of *Concursus Realis* in handling cybercrime cases, including phishing. This principle allows law enforcement to impose the heaviest or maximum penalty for all offenses committed by the perpetrator. However, it is important to note that the prison sentence imposed should not exceed the maximum and heaviest penalty, plus one-third of that limit. This strict punishment approach aims to create a deterrent effect on cybercriminals, thereby reducing the prevalence of phishing and other forms of cybercrimes. Moreover, it serves as an integral part of a broader strategy to prevent cybercrimes. By ensuring the perpetrators of illegal activities receive penalties commensurate with their actions, the legal system plays a role in building a safer and more trustworthy digital environment for the Indonesian population. Thus, the application of strict and proportionate sanctions in phishing cases is a key element in efforts to create a robust and effective legal framework in addressing cybercrime threats in today's digital era.

Overall, the analysis of the ITE Law related to the criminal acts of electronic transactions, such as carding and phishing, shows the need to update and elaborate on regulations related to carding. The current regulations do not fully accommodate technological developments and the types of crimes in the online world. Moreover, prevention and mitigation strategies, both penal and non-penal, are crucial. Penal efforts such as strict law enforcement against computer crime, including carding, are necessary to deter perpetrators. Additionally, non-penal efforts such as public education and training to enhance awareness and safety in online transactions are vital. Collaboration between various stakeholders, including the government, legal experts, academics, the technology industry, and cybersecurity institutions, will be key in developing more specific and detailed regulations related to carding. Furthermore, measures such as the establishment of oversight bodies and international cooperation can help minimize and prevent online crimes. Society should continue to feel safe and comfortable shopping online and enjoy the benefits of technology. Through the implementation of these concrete steps, it is expected that Indonesia can strengthen its defense against carding and similar crimes in the age of advanced technology. With a holistic approach covering regulations, education, and technology, the public can use technology with more confidence and security.

CONCLUSION

Based on the analysis of ITE Law and its relevance to criminal acts of carding and phishing in Indonesia, it can be concluded that the protection of the public from electronic transaction crimes still requires improvement and adjustment to technological developments. The ITE Law contains

provisions that govern criminal acts, such as illegal access to electronic information systems, electronic data theft, and the dissemination of false information through electronic media. However, the existing regulations do not fully accommodate new situations arising with technological advancements, particularly in the context of carding and similar crimes. Therefore, efforts to develop more specific and detailed regulations related to these criminal activities are needed.

The government has strengthened the regulatory framework through Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (P2SK), and Bank Indonesia Regulation No. 3 of 2023 on the Implementation of Payment Transactions (PKBI). These frameworks highlight the state's commitment to ensuring security and data protection in electronic transactions, particularly in the financial sector. The legal sanctions provided by the ITE Law to perpetrators of electronic transaction crimes can include fines and imprisonment, depending on the severity of the crime and the losses incurred. The enforcement of the law related to these criminal acts is carried out by authorized entities such as the police and the Ministry of Communication and Information. Data protection also becomes a crucial concern in carding and phishing, and Indonesia has specific regulations to safeguard personal data.

In the effort to address carding and phishing in online transactions, the government should consider amending the ITE Law to specifically regulate these crimes, providing stronger legal certainty and protection for electronic transaction users. Moreover, financial institutions such as banks and E-Wallet companies, need to improve their security systems. One solution that can be implemented is the use of cryptographic technology, which ensures data authenticity, confidentiality, and user authentication without interference from third parties. In situations where carding occurs, a quick and coordinated response is required. This can be achieved through collaboration between credit card users and relevant e-commerce platforms. Furthermore, specific regulations institutional support are needed to strengthen both software and hardware security systems, reducing vulnerabilities to cyber-attacks. Public awareness also plays a crucial role. Education on safe online practices and the risks of internet use can help prevent carding and phishing, for example avoiding clicking on suspicious links. By implementing these recommendations, it is hoped that the risk of carding and phishing can be minimized, allowing users to conduct a safer and more secure transactions.

REFERENCES

Ali, Erfan Mukhlas, Febrian Dirgantara, and Didit Darmawan. "Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia." *International Journal of Service Science, Management, Engineering, and Technology* 6, no. 3 (2024): 27–38.

Anti-Phishing Working Group (APWG). *Phishing Activity Trends Report*. First Quarter 2025. 2025. https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf.

Anugroh, Y. G, Rommy Hardyansah, Didit Darmawan, Rafadi Khan Khayru, and Arif Rachman Putra. "Consumer Protection and Responsibilities of E-Commerce Platforms in Ensuring the Smooth

Process of Returning Goods in COD Transactions." *Journal of Social Science Studies* 3, no. 2 (2023): 89–94.

Bucy, Erik P, Jordan M Foley, Josephine Lukito, et al. "Performing Populism: Trump's Transgressive Debate Style and the Dynamics of Twitter Response." *New Media & Society* 22, no. 4 (2020): 634–658. https://doi.org/10.1177/1461444819893984.

Butler, Rika. "A Framework of Anti-Phishing Measures Aimed at Protecting the Online Consumer's Identity." *The Electronic Library* 25, no. 5 (2007): 517–533.

CNN Indonesia. "Serangan Phising Meningkat 40 Persen Sepanjang 2023, Cek Targetnya." CNN Indonesia, 2024. https://www.cnnindonesia.com/teknologi/20240313142500-192-1073789/serangan-phishing-meningkat-40-persen-sepanjang-2023-cek-targetnya.

Daim, Tugrul U., Anita Ha, Shawn Reutiman, et al. "Exploring the Communication Breakdown in Global Virtual Teams." *International Journal of Project Management* 30, no. 2 (2012): 199–212. https://doi.org/10.1016/j.ijproman.2011.06.004.

Darmawan, Didit, and E Retnowati. "Peranan Kepercayaan dan Keamanan terhadap Minat Belanja di Tokopedia." *Jurnal Ekonomi Dan Bisnis* 3, no. 1 (2013): 1–6.

Djazilan, Muhammad Sukron, and Didit Darmawan. "The Effect of Religiosity and Technology Support on Trust in Sharia Banking in Surabaya." *Journal of Science, Technology and Society* 2, no. 2 (2021): 7–18.

Firdaus, Rahma Agri. "Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia." *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2025): 79–104. https://doi.org/10.14421/cf582q68.

Firmansyah, Nur Muchammad Ivan, and Luki Nurfanto. "Pertanggung Jawaban Pidana Carding terhadap Pengguna Kartu Kredit." *Mimbar Keadilan* 14, no. 2 (2021): 206–217.

Harris, R B, and D Paradice. "An Investigation of the Computer-Mediated Communication of Emotions." *Journal of Applied Sciences Research* 3, no. 12 (2007): 2081–2090.

Irfan, M, and Dharma S Negara. "The Effectiveness of Consumer Protection Arrangements in E-Commerce Transactions on the Shopee Marketplace Platform in Indonesia." *Journal of Social Science Studies* 3, no. 2 (2023): 115–120.

Kemarauwana, Mukti, and Didit Darmawan. "Perceived Ease of Use Contribution to Behavioral Intention in Digital Payment." *Journal of Science, Technology and Society* 1, no. 1 (2020): 1–4.

Kenny, Charles. "Information and Communication Technologies for Direct Poverty Alleviation: Costs and Benefits." *Development Policy Review* 20, no. 2 (2002): 141–157. https://doi.org/10.1111/1467-7679.00162.

Khairi, Muhammad, and Didit Darmawan. "Blockchain Enforcement in Employee Data Management to Increase Transparency and Security." *International Journal of Service Science, Management, Engineering, and Technology* 7, no. 2 (2025): 1–5.

Manggala, Adi Putra, Kurnia Wijaya, Didit Darmawan, Terubus, and M Syaiful Anwar. "Legal Review of the Implementation of Electronic Contracts and Protection of Parties in Digital Transactions

in Indonesia." *International Journal of Service Science, Management, Engineering, and Technology* 8, no. 1 (2025): 1–8.

Munir, M, R Saputra, P Saktiawan, N H Pakpahan, and F Dirgantara. "Implementation of Consumer Protection Principles in Overcoming the Problem of Ticket Sales by Scalpers through E-Commerce Platforms." *Journal of Social Science Studies* 3, no. 1 (2023): 145–152.

Nurhadi, N, A S Wibowo, Didit Darmawan, Dharma S Negara, and Rommy Hardyansah. "Analysis of Value Added Tax Application on Electronic Commerce Transaction in Digital Economy System in Indonesia." *Journal of Social Science Studies* 3, no. 2 (2023): 83–88.

Okpa, John Thompson, B O Ajah, and J E Igbe. "Rising Trend of Phishing Attacks on Corporate Organisations in Cross River State, Nigeria." *International Journal of Cyber Criminology* 14, no. 2 (2020): 460–478.

Oriento, Dharma S Negara, Arif Rachman Putra, Samsul Arifin, and R Saputra. "Risks and Legal Protection in Non-Cash Financial Transactions through E-Wallets." *Journal of Social Science Studies* 3, no. 1 (2023): 109–114.

Pan, Shan L., and Dorothy E. Leidner. "Bridging Communities of Practice with Information Technology in Pursuit of Global Knowledge Sharing." *The Journal of Strategic Information Systems* 12, no. 1 (2003): 71–88. https://doi.org/10.1016/S0963-8687(02)00023-9.

Putra, Arif Rachman, E Retnowati, Lestari, U P, et al. "Analysis of the Influence of Privacy, Security and Ease of Use on Intention to Shopping through the Marketplace." *Journal of Marketing and Business Research* 3, no. 1 (2023): 35–48.

Setiawan, Daryanto. "Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Budaya." *Jurnal Simbolika Research and Learning in Communication Study* 4, no. 1 (2018): 62–72.

Sinambela, Ella Anastasya, and Didit Darmawan. "Advantages and Disadvantages of Using Electronic Money as a Substitute for Cash." *Journal of Social Science Studies* 2, no. 2 (2022): 56–61.

Vayansky, Ike, and Sathish Kumar. "Phishing – Challenges and Solutions." *Computer Fraud & Security* 2018, no. 1 (2018): 15–20. https://doi.org/10.1016/S1361-3723(18)30007-1.

Wahyudi, W, R N K Kabalmay, and M W Amri. "Big Data and New Things in Social Life." *Studi Ilmu Sosial Indonesia* 1, no. 1 (2021): 1–12.

Warda, Ayesha, and Jhumur Samaddar. "A Primary Study on User Perception of Phishing in Banking Sector." *SJCC Management Research Review*, August 13, 2022, 59–79. https://doi.org/10.35737/sjccmrr/v12/i1/2022/155.