Journal of International Islamic Law, Human Right and Public Policy

Journal of International Islamic Law, Human Rights, and Public Policy (JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 4 No. 3 (2026)

MISUSE OF TAXPAYER DATA FOR PHISING SCAMS

Nuradi Budi Prakoso[1], Hanuring Ayu[2], Hafid Zakaria[3]
Universitas Islam Batik Surakarta

Received: 03/06/2026 | **Revised:** 08/06/2026 | **Accepted:** 20/06/2026 | **Published:** 20/07/2026

Abstract

The rapid development of Indonesia's digital taxation ecosystem has simultaneously introduced new vulnerabilities that were previously absent in conventional tax administration systems. This research examines the misuse of taxpayer data as the primary instrument in phishing schemes, a phenomenon that not only inflicts financial and psychological harm on individual victims, but also erodes public trust in tax institutions and undermines the broader success of digital government transformation. This study employs a juridical-empirical method with a descriptive-analytical character, integrating statutory and conceptual approaches. The research yields three principal findings. First, taxpayer data occupies a uniquely strategic position as information collected under legal obligation, simultaneously encompassing identity, financial, and asset data, making it a high-value target whose misuse erodes the public trust that underpins Indonesia's self-assessment taxation paradigm. Second, the misuse of taxpayer data in phishing practices occurs through five primary modes, namely counterfeit website creation, mass deceptive messaging, malicious application distribution, voice phishing, and spear phishing, all of which exploit a five-phase exploitation chain and employ psychological manipulation techniques grounded in institutional authority, artificial urgency, and data-driven personalization. Third, the effectiveness of existing regulations, including the Electronic Information and Transactions Law, Law Number 27 of 2022 on Personal Data Protection, and the General Tax Provisions Law, remains insufficient due to fragmentation of legal substance, limited institutional enforcement capacity, and low legal awareness among taxpayers. This research recommends the accelerated operationalization of the Personal Data Protection Authority, the establishment of an integrated cross-institutional phishing detection and response system, and the strengthening of international legal cooperation as integral components of a systemic and sustainable data protection strategy.

Keywords: phishing, taxpayer data, personal data protection, cybercrime, digital tax administration.

INTRODUCTION

The current digital era, which demands the transformation of public services into information technology platforms, has brought both convenience and serious challenges, particularly in the field of taxation. The Directorate General of Taxes (DJP) of the Republic of Indonesia continues to promote the digitalization of its services through online systems, such as DJP Online and the M-Pajak application, with the aim of accelerating public services and improving taxpayer compliance. However, this growth has also been accompanied by the increasing prevalence of cybercrime targeting personal and tax-related data (Arif et al. 2024). This phenomenon is crucial because tax data are not merely administrative figures but sensitive information containing taxpayer identities and financial aspects that can be misused for criminal purposes if they fall into the wrong hands. This phenomenon has been reflected in various warnings and phishing incidents impersonating DJP to deceive taxpayers into disclosing their data through fraudulent links or messages that appear official but are actually malicious (Gumay, Hendrawan, and Kusumah 2024). These phishing attempts demonstrate how perpetrators exploit public trust in government institutions to influence taxpayer behavior, resulting in potential personal losses as well as systemic weaknesses in the protection of state data (Lukito and Handaya 2025). Such cases highlight the importance of academic research on the misuse of taxpayer data within the increasingly complex and organized landscape of cybercrime. The misuse of taxpayer data through phishing is one manifestation of technology-based crime, reflecting underlying issues related to information security vulnerabilities and low levels of digital awareness among the public(V. F. Putra 2021). Phishing is a fraudulent technique that attempts to obtain victims' sensitive information, such as identity, account credentials, and passwords, by impersonating a trusted entity in digital communications(Puspitasari and Sutabri 2023). In various

countries, this phenomenon has caused significant impacts. For example, in the United Kingdom, approximately 100,000 taxpayer accounts were affected by phishing, resulting in financial losses amounting to tens of millions of pounds due to fraudulent tax refund claims made by criminals using stolen identity data(Fadli, Widijowati, and Andayani 2024).This incident illustrates that even advanced tax systems can become major targets for data misuse through phishing attacks. Such cases demonstrate that phishing is a cross-border threat involving organized perpetrators capable of exploiting minor data exposures into substantial collective losses.

In Indonesia, various phishing schemes impersonating DJP illustrate how criminals send messages via WhatsApp, e-mail, or fraudulent websites to lure taxpayers into providing their personal data and account credentials. These methods include sending links that imitate official DJP domains, requesting data updates through malicious applications, and making false claims regarding tax arrears or tax refunds that must be claimed immediately(Anjheli 2024). These facts indicate that, in addition to external threats to the system, problems also arise from taxpayers' limited understanding and awareness of digital manipulation techniques, making it easier for perpetrators to exploit the data they possess.(Wiranata et al. 2024) Frequently, the messages appear highly convincing because they use formal language, official logos, and information genuinely related to taxpayer data, indicating that phishing perpetrators already possess preliminary access to victims' personal information before initiating the fraud.(Kelas and Iskandar 2024)

The root causes of taxpayer data misuse are highly complex, consisting of a combination of weaknesses in digital security, limitations in regulations specifically addressing cybercrimes such as phishing, and low levels of digital literacy within society. From a technological perspective, tax service platforms remain vulnerable if they are not equipped with robust security mechanisms and continuous monitoring against domain imitation attempts and phishing campaigns. (Nervia et al. 2025) From a legal perspective, although Indonesia has enacted laws governing electronic information and personal data protection, challenges remain in their effective implementation to address evolving forms of digital fraud that continuously exploit regulatory gaps(Ahmadian and Sabri 2021). From a social perspective, many taxpayers still lack an adequate understanding of official digital tax service mechanisms, making them susceptible to systematic manipulation schemes designed by cybercriminals. (Purnamasari and Sutabri 2023)

Addressing this issue within an academic context requires a multidimensional analysis encompassing technical, legal, and social aspects. Technically, research may examine how phishing exploits weaknesses in online communication and identify the attack techniques used to gain access to taxpayer data. Legally, research should evaluate the strengths and weaknesses of existing regulations in providing personal data protection as well as the effectiveness of law enforcement against phishing perpetrators. Socially, this approach should assess taxpayers' understanding and behavior when interacting with digital tax systems and identify effective educational strategies to enhance public awareness and the ability to recognize phishing threats. Through a comprehensive, evidence-based approach, this research is expected to provide an overall understanding of the phenomenon of taxpayer data misuse for phishing crimes and offer practical policy recommendations to strengthen the tax data security ecosystem in Indonesia.

This research aims to comprehensively examine the patterns of taxpayer data misuse in phishing crimes by positioning the phenomenon within the broader context of the digital transformation of tax administration services. Through empirical analysis, this research seeks to generate new insights into how taxpayer data are exploited in phishing schemes, from the initial acquisition of data to the manipulation of victims, thereby identifying critical points of vulnerability that have previously received limited attention. Furthermore, this research aims to assess the effectiveness of the legal framework and policies governing the protection of taxpayer data in addressing the continuously evolving threat of phishing. This assessment focuses not only on the existence of regulations from a normative perspective but also on their implementation, inter-agency coordination, and practical responses to cases of data misuse. Accordingly, this research is expected to produce new findings regarding the gap between existing regulations and the reality of cybercrime in the taxation sector. Another objective of this research is to formulate more adaptive prevention and mitigation approaches by integrating technological, legal, and taxpayer digital literacy aspects. This approach is expected to generate conceptual and practical recommendations that are not only reactive to phishing incidents but also preventive in strengthening the resilience of the digital taxation system. Through these objectives, the research seeks to contribute to the development of a more contextual and responsive model for taxpayer data protection against contemporary cybercrime challenges.

METHOD

This research is a legal study employing an empirical-juridical approach with a descriptive-analytical nature. Legal research is used because the issues examined are directly related to legal norms, public policy, and the protection of taxpayer data within the digital taxation system. The descriptive-analytical(Abdussamad 2021) approach is chosen

to comprehensively describe the phenomenon of taxpayer data misuse in phishing practices while analyzing the relationship between the applicable legal norms and the empirical realities. Through this approach, the research does not merely present facts but also provides a critical analysis of the effectiveness of the existing legal protection and its implications for taxpayers' rights. The data sources in this research consist of primary and secondary data. Primary data are obtained from empirical facts related to phishing practices impersonating tax institutions, including taxpayers' experiences, field findings, and information from parties who understand the management and protection of tax data. Secondary data are obtained from primary legal materials in the form of relevant legislation, secondary legal materials in the form of books, scientific journals, previous research, and policy documents discussing cybercrime, personal data protection, and the digital taxation system. In addition, non-legal materials such as official reports, institutional publications, and supporting academic sources are used to enrich the analysis.

Data collection is conducted through literature study and selective empirical data collection. The literature study is carried out by reviewing and examining legislation, academic literature, and research findings relevant to the research topic. (Abdussamad 2021). Empirical data collection is conducted to obtain a realistic understanding of phishing practices and taxpayer data misuse through case tracing, documentation, and information obtained from relevant parties. These data collection methods are selected to ensure that the research has a strong normative foundation while also being supported by empirical realities. (Widodo et al. 2023) Data analysis in this research is conducted qualitatively using a balanced combination of inductive and deductive reasoning. The collected data are analyzed by classifying, relating, and interpreting information relevant to the research focus. (Creswell and Creswell 2018). Normative analysis is used to assess the adequacy and suitability of regulations in protecting taxpayer data, while empirical analysis is used to understand patterns of data misuse and the factors influencing them. The results of the analyses are then synthesized to produce research findings in the form of problem mapping, a conceptual model for taxpayer data protection, and practical policy recommendations based on actual needs.

RESULTS AND DISCUSSION

A. Coretax Scam and the Risks of Data Breaches

Through Announcement Number PENG-4/PJ.09/2025 concerning Beware of Fraud Impersonating the Directorate General of Taxes, DJP emphasizes that phishing cases have indeed occurred in Indonesia, where fraudsters impersonate DJP officials through telephone calls, emails, or text messages to manipulate victims into providing their personal information. An article published by Katadata.co.id describes the increasingly sophisticated cyber threats in Indonesia, focusing on the misuse of the integrated tax administration system, Coretax. This type of fraud illustrates how leaked personal data can be manipulated to systematically drain victims' funds.

This crime begins with psychological exploitation, in which perpetrators impersonate tax authorities. By mentioning accurate personal information such as the National Identity Number (NIK) and Taxpayer Identification Number (NPWP), the perpetrators successfully lower the victims' vigilance. The urgency of the Annual Tax Return (SPT Tahunan) filing period in March is used as an opportunity to pressure victims into downloading fake applications and enabling screen-sharing features, ultimately leading to the theft of their banking credentials.

Large-scale data breaches that end up on the dark web serve as the primary source for social engineering attacks. Such data enhance the credibility of fraudulent schemes, making it increasingly difficult to distinguish between legitimate and fraudulent communications. Fraud schemes disguised as Coretax demonstrate that digital security is not solely a matter of technological infrastructure but also of effective data governance and user literacy. As long as personal data remain easily accessible to unauthorized parties, the risk of digital fraud will continue to be high in Indonesia.

B. The Transformation of Taxpayer Data: From a State Administrative Instrument to a Tool of Crime that Undermines Public Trust

Taxpayer data occupy a unique and strategic position within the architecture of the state's financial administration. Unlike personal data collected by private business entities based on contractual agreements, taxpayer data are collected pursuant to legal obligations imposed on every individual and business entity that meets the criteria of a tax subject. (Malendes, Sabijono, and Weku 2024) The obligation to provide such data is not voluntary but is grounded in the state's sovereignty to manage fiscal revenue for financing government administration and national development. Within this framework, the state acts not merely as the recipient of information but also as the trustee fully responsible for ensuring the security and confidentiality of the data entrusted to it. Law Number 28 of 2007 concerning General Provisions and Tax Procedures, as amended several times, most recently by Law Number 7 of 2021 concerning the Harmonization of Tax Regulations, explicitly provides that all data and information submitted

by taxpayers to DJP are confidential. Article 34 of the General Tax Provisions Law requires tax officials to maintain the confidentiality of such data and prohibits its disclosure to other parties except for purposes permitted by law. This prohibition is not merely an internal ethical standard within the bureaucracy but a legal norm that may result in criminal sanctions for violations, reflecting the seriousness with which the state regards the protection of taxpayer data as a constitutional obligation.

Substantively, taxpayer data contain information that is far more comprehensive than ordinary personal data. Such data include not only basic identity information such as names, addresses, and National Identity Numbers (NIK), but also Taxpayer Identification Numbers (NPWP), income profiles from various sources, information on movable and immovable assets, financial account data, tax compliance histories, and affiliation relationships with other entities within business networks. The richness of this information makes taxpayer data highly valuable not only for fiscal authorities in ensuring fair tax collection but also for criminals who recognize its potential for exploitation.

Understanding how taxpayer data are transformed into instruments of crime requires examining the channels through which such data move from the state's management domain into the hands of criminals. This research identifies at least four primary channels that have empirically been shown to facilitate the misuse of tax-related data. First, data breaches originating from within the tax administration system due to weaknesses in information security, human error, or insider threats involving rogue officials. Second, data breaches resulting from the exploitation of technical vulnerabilities in digital tax service platforms such as DJP Online and the M-Pajak application. Third, indirect acquisition of data through the reconstruction of publicly available information combined with data obtained from breaches originating from other sources. Fourth, active data theft through social engineering attacks targeting taxpayers directly.

The fourth channel constitutes the core phenomenon of phishing examined in this research. In this scenario, perpetrators do not directly attack DJP systems but instead exploit taxpayers' trust in the tax authority to persuade them to voluntarily disclose sensitive information. The success of this strategy depends largely on how effectively the perpetrators imitate the identity and authority of DJP, how convincing the fraudulent scenario appears, and how limited the victim's awareness is regarding potential fraud. Notably, the most effective phishing perpetrators often already possess partial taxpayer information before launching their attacks, making their fraudulent communications appear highly personalized and credible.

The theory of cognitive manipulation developed by Robert Cialdini in his research on influence and persuasion provides a highly relevant framework for understanding why phishing attacks impersonating tax authorities are so effective. Cialdini identifies the principle of authority as one of the strongest triggers of compliance in human psychology: individuals tend to follow instructions from parties perceived to possess legitimate authority without engaging in extensive critical verification. (Putri et al. 2023) Tax institutions, with their symbols of authority, formal language, and executive powers, represent an ideal manifestation of authority that can be exploited by phishing perpetrators. The combination of the authority principle and the scarcity principle—emphasizing that immediate action is required or serious consequences will follow—creates psychological conditions that are highly susceptible to fraud.

The transformation of taxpayer data into an instrument of crime does not occur through a single step but rather through a series of interconnected stages. In the first stage, perpetrators conduct reconnaissance to collect preliminary information about potential victims, including names, addresses, NPWP, and other basic information available from various sources. In the second stage, this information is used to establish the credibility of fraudulent communications so that victims become less suspicious. In the third stage, victims are encouraged to take specific actions that result in the disclosure of more sensitive information or access to more valuable systems. In the fourth stage, the acquired data are exploited for subsequent criminal purposes, including direct financial fraud, the sale of data on the black market, or their use as resources for launching more sophisticated phishing attacks.

The impact of taxpayer data misuse extends beyond the losses suffered by individual victims and reaches a more fundamental dimension concerning public trust in state institutions. In the context of taxation, public trust holds significant strategic value because modern tax systems in nearly all countries, including Indonesia, are based on the principle of self-assessment, which requires voluntary taxpayer compliance. (Fahmi and Hari 2023). Such voluntary compliance can only be achieved when taxpayers trust that the data they provide to the state will be securely managed, protected from misuse, and kept out of the hands of unauthorized parties. When this trust is eroded by repeated phishing incidents, the motivation for voluntary compliance also tends to decline. (I. K. O. K. Putra et al. 2022).

Research in fiscal psychology developed by Erich Kirchler and his colleagues through the Slippery Slope Framework demonstrates that the relationship between taxpayers and tax authorities is influenced by two key variables: trust and power. (I. K. O. K. Putra et al. 2022) When trust is high and governmental authority is perceived positively, taxpayers are more likely to comply voluntarily. Conversely, when trust declines, compliance becomes increasingly coercive and depends primarily on law enforcement. Phishing incidents impersonating tax authorities, if not properly addressed, may systematically shift public perception from trust to distrust, thereby imposing substantially greater compliance costs on the tax enforcement system in the long term.

Furthermore, phishing based on taxpayer data also threatens the integrity of the ongoing digital transformation of Indonesia's tax administration. Through DJP, Indonesia has made significant investments in developing a digital tax ecosystem, including electronic tax return filing, online tax payment services, and the development of the Coretax Administration System, which is expected to become the next-generation digital tax infrastructure. The success of this digital transformation depends heavily on user adoption and public trust. Every successful phishing incident exploiting the identity of DJP not only causes direct losses to victims but also creates doubts regarding the security of digital tax platforms as a whole, which may ultimately hinder the adoption of digital services and reduce the efficiency of the national tax system.

An analysis of several documented phishing cases reveals a consistent pattern: perpetrators consistently exploit specific moments associated with the tax cycle, such as the approach of the annual tax return filing deadline, tax audit periods, or the introduction of new tax policies receiving widespread media attention. The careful selection of these moments reflects the perpetrators' deep understanding of the tax calendar and taxpayers' psychological conditions during these periods, demonstrating that taxpayer data-based phishing is not merely an opportunistic crime but rather a planned and organized activity with an increasingly sophisticated level of execution.

C. Patterns of Taxpayer Data Misuse in Phishing Practices: Modus Operandi, Data Acquisition Process, and Psychological Manipulation Techniques

The modus operandi of phishing targeting taxpayer data has evolved significantly alongside the increasing digital literacy of cybercriminals and the growing sophistication of digital communication infrastructure. This research identifies five primary methods consistently found in various reports and empirical findings from both government institutions and the national cybersecurity community.

The first method involves the creation of fraudulent websites that are visually almost identical to the official DJP portal, namely www.pajak.go.id or the DJP Online platform. This technique, commonly known as website spoofing, exploits users' tendency to judge the authenticity of a website based on its appearance rather than on technical indicators that are more difficult to recognize, such as digital certificates and domain validity. Perpetrators employ typosquatting by registering domain names that closely resemble the official domain, such as *pajak-go.id*, *djp-online.id*, or *pajakgo.id*, which can easily be mistaken for the legitimate domain at a glance. These fraudulent websites are then equipped with forms requesting taxpayers to enter their NPWP, passwords, personal identity information, and even bank account details under the pretext of account verification or data updates.

The second method is the distribution of mass phishing messages through various digital communication channels, including e-mail, WhatsApp, SMS, and even social media. These messages generally use templates designed to create urgency and anxiety among recipients, with content ranging from claims of outstanding tax liabilities requiring immediate payment, notifications of tax refunds that will expire if not claimed within a specified period, to warnings regarding the suspension of NPWP due to non-compliance with tax reporting obligations. What distinguishes this method from ordinary phishing is the use of genuine taxpayer information, such as full names and NPWP, to make the communication appear personal and convincing, thereby reducing the likelihood that victims will recognize the messages as fraudulent.

The third method involves the distribution of fake applications that imitate the appearance of DJP's official M-Pajak application. These applications are distributed through download links sent via text messages or social media or uploaded to third-party application repositories that lack strict verification mechanisms. Once installed on the victim's device, the fake application may secretly collect data, record keystrokes to steal passwords, or even gain access to all information stored on the device. This method is particularly dangerous because victims are often unaware of the data breach until substantial losses have already occurred.

The fourth method is voice phishing (vishing), in which perpetrators contact taxpayers by telephone while impersonating DJP officials or even law enforcement officers. In this scenario, the perpetrators exploit perceived authority by using formal language, demonstrating prior knowledge of certain taxpayer information, and constructing scenarios that create intense psychological pressure. Taxpayers who are inexperienced or unfamiliar with DJP's

official communication procedures are particularly vulnerable to this method because direct voice interaction tends to reduce the time available for critical thinking while increasing compliance with the perpetrator's instructions.

The fifth method is spear phishing, which specifically targets selected taxpayers, generally business owners, corporate executives, or high-income individuals whose tax information possesses greater economic value. Unlike mass phishing, which is broad and indiscriminate, spear phishing employs a highly personalized approach by utilizing background information about the target collected from various sources before the attack is launched. The success rate of spear phishing is significantly higher than that of mass phishing because its personalized nature makes the messages appear highly legitimate and relevant to the recipient.

Understanding the process through which data are obtained in tax-related phishing schemes is essential for designing effective protection strategies, as appropriate intervention points can only be identified when the entire chain of criminal activity is carefully mapped. The success of phishing as a cybercrime method does not depend solely on the sophistication of the technology employed but is largely determined by the effectiveness of the psychological manipulation directed at victims. Understanding the psychological mechanisms exploited in tax-related phishing is therefore a prerequisite for developing truly effective protection strategies, as even the most advanced technical solutions will remain inadequate if the human dimension of this crime is not properly addressed.

D. The Effectiveness of Regulations in Preventing and Addressing Phishing Targeting Taxpayer Data

Addressing phishing targeting taxpayer data requires a careful analysis of the existing regulatory landscape, including the identification of relevant legal instruments, the mapping of the scope of protection they provide, and a critical evaluation of the regulatory gaps that remain. Indonesia has established several legal instruments that can partially be used to combat this type of cybercrime, although none specifically and comprehensively regulates phishing in the context of taxpayer data.

Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 and subsequently by Law Number 1 of 2024, serves as the principal legal instrument governing cybercrime in Indonesia. Article 28 paragraph (1) prohibits the dissemination of electronic information containing false and misleading information that causes consumer losses in electronic transactions, which is directly relevant to phishing activities. Article 30 prohibits unauthorized access to another person's electronic system, including data theft through fraudulent websites or malicious applications. Article 35 regulates the manipulation of electronic documents, which is relevant to the falsification of DJP's visual identity in phishing websites and messages. Nevertheless, these provisions are formulated in general terms and do not specifically distinguish the strategic value and sensitivity of taxpayer data from digital data in general.

Law Number 27 of 2022 concerning Personal Data Protection is the most recent and comprehensive legal instrument governing data protection in Indonesia. This law explicitly recognizes the rights of data subjects, establishes the obligations of data controllers, regulates the processing of sensitive personal data under higher standards, and provides both administrative and criminal sanctions for violations. The provisions concerning the unauthorized processing of personal data and the obligation to notify data breaches are directly relevant to phishing involving taxpayer data. However, the principal challenge in implementing this law is that the supervisory authority mandated by the legislation, namely the Personal Data Protection Agency, was still in the process of being established and had not yet become fully operational at the time this research was conducted. Consequently, the implementation of the law's key provisions remains limited.

Law Number 28 of 2007 concerning General Provisions and Tax Procedures, particularly Article 34, provides protection for the confidentiality of taxpayer data held by the tax authority. This provision requires every tax official to maintain the confidentiality of all information obtained from or provided by taxpayers in the course of their official duties. Violations of this obligation may result in imprisonment and substantial fines. However, this provision is primarily designed to protect against internal threats, namely the misuse of taxpayer information by tax officials themselves, and does not specifically regulate external threats such as phishing perpetrators who exploit taxpayer data from outside the DJP system.

The existence of these relatively comprehensive legal instruments does not automatically guarantee effective protection against phishing targeting taxpayer data in practice. According to Lawrence Friedman in his legal system theory, the effectiveness of law is determined by three interacting components: legal structure, legal substance, and legal culture. These three components must be evaluated separately to obtain a comprehensive understanding of why significant protection gaps remain despite the existence of adequate legal instruments at the normative level. (Basha 2024).

From the perspective of legal substance, the principal issue identified is the fragmentation of regulations across multiple legal instruments without an effective mechanism for integration. Each legal instrument governs a particular aspect of the problem, yet no single regulation holistically addresses the protection of taxpayer data against phishing as an integrated issue. This condition creates what legal scholars often describe as overlapping jurisdiction, where multiple institutions consider themselves to possess authority, but none assumes full responsibility. As a result, responses to phishing incidents involving taxpayer data are frequently slow, poorly coordinated, and ineffective. (Heriana et al. 2023).

From the perspective of legal structure, the challenges relate to institutional capacity that has not kept pace with the complexity and scale of the threat. The Cyber Crime Directorate of the Criminal Investigation Agency (Bareskrim Polri), as the primary law enforcement unit for cybercrime, faces limitations in trained human resources, adequate digital forensic capabilities, and operational coverage that remains largely concentrated at the national level. In addition, coordination among Bareskrim, DJP, the National Cyber and Crypto Agency (BSSN), and the Financial Services Authority (OJK) in handling taxpayer data phishing cases remains largely incidental and has not yet been supported by structured and binding coordination mechanisms.

From the perspective of legal culture, the most fundamental challenge is the limited awareness among taxpayers regarding their data protection rights and the available mechanisms for enforcing those rights. Many taxpayers who become victims of phishing do not report the incidents to the relevant authorities because they are unaware of the reporting procedures, lack confidence that reporting will lead to satisfactory resolution, or fear that lengthy legal proceedings will cause greater inconvenience than the losses already suffered. This situation creates a significant dark figure of crime(Wijaya et al. 2024) in taxpayer phishing statistics, which in turn deprives policymakers of an accurate understanding of the true scale of the problem.

Law enforcement challenges are further complicated by the cross-border nature of phishing crimes. Perpetrators targeting Indonesian taxpayers frequently operate through servers located abroad while concealing their identities using VPNs, TOR networks, or other anonymization services. Identifying, tracing, and extraditing perpetrators from foreign jurisdictions requires complex and time-consuming international legal cooperation mechanisms, while the digital evidence required for prosecution is often volatile, making it susceptible to alteration, disappearance, or deletion before legal proceedings can be initiated. These limitations make cross-border phishing cases among the most difficult law enforcement challenges to resolve in the short term.

The evaluation of the existing regulatory framework identifies several significant gaps that must be addressed to strengthen the protection of taxpayer data against phishing threats. These gaps are neither simple nor capable of being resolved through a single intervention; rather, they require a systematic and multi-layered approach.

The first gap is the absence of regulations that specifically govern the protection of taxpayer data against phishing as a distinct category of crime. This regulatory vacuum results in the lack of clear response standards when phishing incidents occur, the absence of structured notification obligations for taxpayers who may be affected, and the lack of standardized recovery mechanisms for victims. This gap may be addressed through the issuance of more specific implementing regulations under the framework of the Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (ITE Law), or through the formulation of joint technical regulations by the Ministry of Finance, the Ministry of Communication and Information Technology, and the Indonesian National Police.

The second gap is the inadequacy of cyber threat information-sharing mechanisms among DJP, the National Cyber and Crypto Agency (BSSN), Bareskrim, and banking institutions. In an effective cybersecurity ecosystem, information regarding emerging attack patterns should be shared rapidly among all relevant stakeholders so that preventive measures can be implemented before attacks reach a harmful scale. The absence of a structured and routinely implemented information-sharing mechanism is one of the reasons why tax-related phishing websites and applications often remain operational for considerable periods before they are detected and taken down.

The third gap is the lack of provisions establishing minimum security standards that must be implemented by DJP in managing and delivering digital communications to taxpayers. The technical standardization of official DJP communications, including the use of verified domains, end-to-end encryption, digital signatures for official electronic correspondence, and two-factor authentication for all access to DJP Online and Coretax, represents technical measures that could substantially reduce the ability of perpetrators to create convincing fraudulent communications. In response to these identified gaps, this research proposes several constructive recommendations based on an in-depth analysis of the underlying problems. From a legislative perspective, there is a need to formulate technical regulations specifically governing taxpayer data protection standards within the digital tax ecosystem, including the obligation for DJP to implement early detection systems for the unauthorized use of its identity in

cyberspace. These regulations should ideally be developed collaboratively by DJP, the Ministry of Communication and Information Technology, BSSN, and cybersecurity experts from both academia and industry. From an institutional perspective, there is a need to establish a permanent coordination mechanism involving all relevant institutions, with a clear mandate to share threat intelligence in real time, coordinate responses to incidents, and periodically report the progress of case handling to the public. This mechanism does not necessarily require the creation of a new institution, which would involve considerable time and expense, but may instead be established through an inter-agency task force supported by a strong legal foundation and standardized operational procedures.

From the perspective of taxpayer empowerment, comprehensive, sustainable educational programs are needed, based on an empirical understanding of the knowledge gaps most vulnerable to exploitation by phishing perpetrators. Such programs should not be limited to distributing pamphlets or posting information on social media but should instead be designed as measurable behavioral interventions using communication methodologies proven effective in improving taxpayers' awareness and their ability to verify communications claiming to originate from DJP. Although investment in public education may not produce immediate results, it represents one of the most cost-effective long-term strategies for preventing phishing.

From the perspective of protecting victims' rights, more accessible recovery mechanisms should be developed without burdening victims with lengthy and complicated procedures. The establishment of integrated complaint services accessible through multiple channels, simplified and standardized compensation mechanisms, and access to legal assistance for victims in need are essential components of a comprehensive protection system that responds to the practical needs of taxpayers as the parties most vulnerable within the tax-related phishing ecosystem.

Overall, the findings of this research demonstrate that phishing targeting taxpayer data is a multidimensional issue that cannot be addressed through a sectoral approach alone. A consistent commitment from all stakeholders is required to establish a protection system that is not only comprehensive in its normative framework but also effective in its implementation. Only through such an approach can taxpayer data be restored to its proper function solely as a state administrative instrument serving the collective fiscal interest, rather than remaining vulnerable to exploitation as a tool of crime that harms individuals while undermining public trust in state institutions.

CONCLUSION

This research has comprehensively examined the issue of taxpayer data misuse for phishing crimes from three interrelated dimensions, namely the function and position of taxpayer data within the state administrative system, the patterns of crime in empirical practice, and the effectiveness of regulations and law enforcement. Based on the overall analysis, this research arrives at three principal conclusions that reinforce one another and collectively provide a comprehensive understanding of the issue under study.

First, taxpayer data occupy a unique and strategic position within Indonesia's digital information ecosystem because they are collected pursuant to legal obligations, managed by the state, and contain information that is far more comprehensive than ordinary personal data. This uniqueness makes taxpayer data an especially attractive target for cybercriminals, as they include not only basic identity information but also financial profiles, asset ownership records, and tax compliance status, enabling the creation of highly personalized and convincing fraudulent schemes. The transformation of taxpayer data from a state administrative instrument into a tool of crime occurs through various channels, originating both from weaknesses within the DJP system and from perpetrators' active exploitation of taxpayers' trust in the tax authority. The consequences of this transformation are multidimensional: at the individual level, they result in financial and psychological harm, while at the institutional level, they erode public trust in the digital tax system currently undergoing transformation. This erosion of public trust directly threatens the success of the self-assessment system that forms the foundation of Indonesia's taxation system, as voluntary taxpayer compliance depends largely on confidence that the state is capable of protecting the data entrusted to it.

Second, the pattern of taxpayer data misuse in phishing practices demonstrates an increasing level of sophistication and can no longer be regarded merely as opportunistic crime. This research identifies five principal methods operating through distinct approaches, ranging from the creation of fraudulent websites, the distribution of mass phishing messages, and malicious applications to voice phishing through telephone calls and highly personalized spear phishing attacks. Each method employs a combination of social engineering techniques designed to exploit taxpayers' psychological vulnerabilities, particularly through the manipulation of institutional authority, the creation of artificial urgency, the induction of fear concerning potential legal consequences, and the personalization of communications using previously acquired data. The exploitation chain identified in this research consists of five sequential and interdependent stages: reconnaissance, infrastructure preparation, attack execution,

data extraction, and monetization. Understanding this exploitation chain is essential because it provides a clear framework for identifying the most effective intervention points to disrupt criminal activities before irreversible harm occurs.

Third, the effectiveness of the existing regulatory framework in preventing and addressing phishing targeting taxpayer data remains inadequate, despite Indonesia's possession of several relevant legal instruments at the normative level. An analysis based on Friedman's legal system theory reveals deficiencies across all three components of the legal system simultaneously. From the perspective of legal substance, there is no regulation that specifically and comprehensively governs the protection of taxpayer data against phishing as an integrated legal issue, requiring law enforcement authorities to rely on a combination of provisions from multiple statutes, resulting in inconsistent implementation. From the perspective of legal structure, institutional capacity remains limited, inter-agency coordination continues to be largely incidental, and formal mechanisms for sharing cyber threat information have yet to be systematically established. From the perspective of legal culture, taxpayers' awareness of their data protection rights and available reporting mechanisms remains low, resulting in a significant dark figure of crime a criminological term referring to crimes that are not reported to the police or recorded in official statistics which in turn deprives policymakers of accurate data regarding the true scale of the problem.

REFERENCES

Abdussamad, Zuchri. 2021. *Metode Penelitian Kualitatif*. Edited by Patta Rapanna. 1st ed. @Syakir Media Press.

Ahmadian, Hendri, and Aulia Sabri. 2021. "TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA." *Djtechno* 2 (1): 13–20.

Anjheli, Devi. 2024. "Privasi Digital Dan Kejahatan Phishing Di Indonesia: Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP." *STAATSRECHT* 4 (1): 165–89.

Arif, Muhammad, Bagus Dewanto, Muhammad Fathurrahman, Danar Restu Firdaus, and Aep Setiawan. 2024. "Penipuan Penambah Followers Instagram : Analisis Serangan Phising Dan Dampaknya Pada Keamanan Data." *Journal of Internet and Software Engineering* 1 (4): 1–11.

Basha, Syed Hayath. 2024. "HUMAN RIGHTS EDUCATION : CURRENT ISSUES AND POSSIBLE SOLUTIONS." *Journal of AKCE* 2 (2): 17–28.

Creswell, John W., and J. David Creswell. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth Edit. Californi: SAGE Publications, Inc.

Fadli, Muhammad, Dijan Widijowati, and Dwi Andayani. 2024. "Pencurian Data Pribadi Di Dunia Maya (Phising Cybercrime) Yang Ditinjau Dalam Perspektif Kriminologi." *Co-Value* 14 (12): 824–36.

Fahmi, Muhammad, and Kurnia Krisna Hari. 2023. "KUALITAS PELAYANAN DAN SANKSI PERPAJAKAN TERHADAP KEPATUHAN WAJIB PAJAK ORANG PRIBADI DI KPP ILIR TIMUR KOTA PALEMBANG." *BALANCE* 8 (2): 164–74.

Gumay, Berlyan, Ade Hendri Hendrawan, and Fitrah Satrya Fajar Kusumah. 2024. "ANALISIS DAMPAK ANCAMAN CYBERCRIME TERHADAP DATA MAHASISWA PADA SERANGAN WEB PHISING SIAK UIKA." *INFOTECH* 10 (2): 297–305.

Heriana, Kamiliya M A, Raisha A Rismarina, Audithya Prawita, Jagad Satrio Hussein, and Ferry Irawan. 2023. "ANALISIS MANAJEMEN PAJAK PADA PERUSAHAAN MANUFAKTUR : STUDI KASUS PT OMG." *EDUCORETAX* 3 (4): 286–300.

Kelas, and Octo Iskandar. 2024. "Analisis Kejahatan Online Phishing Pada Masyarakat." *Leuser* 1 (2): 32–36.

Lukito, and Wilfridus Bambang Triadi Handaya. 2025. "Deteksi Website Phishing Menggunakan Teknik Machine Learning." *Informatika Atma Jogja* 6 (1): 69–80.

Malendes, Daniel, Harijanto Sabijono, and Pricillia Weku. 2024. "Pengaruh Pengetahuan Perpajakan, Kesadaran Wajib Pajak Dan Sanksi Pajak Terhadap` Kepatuhan Wajib Pajak Dalam Membayar Pajak Bumi Dan Bangunan Di Kecamatan Pulau Batang Dua Kota Ternate." *Riset Akuntansi Dan Portofolio Investasi* 2 (2): 93–100. https://doi.org/10.58784/rapi.131.

Nervia, Clara, Kresentia Aiko Wardhana, Pricilia Angel Sie, Talitha Livia Talim, and Waynehard Brayne Hizkia. 2025. "ANALISIS YURIDIS TERHADAP KEJAHATAN PHISING DALAM SISTEM PERBANKAN DIGITAL MELALUI SCAM LINK BERBAHAYA." *IKON* 29 (2): 13–30.

Purnamasari, and Tata Sutabri. 2023. "Analisis Kejahatan Online Phising Pada Institusi Pemerintah / Pendidik Sehari-Hari." *JURNAL DIGITAL TEKNOLOGI INFORMASI* 06 (01): 29–34.

Puspitasari, Devi, and Tata Sutabri. 2023. "Analisis Kejahatan Phising Pada Sektor E-Commerce Di Marketplace Shopee." *JURNAL DIGITAL TEKNOLOGI INFORMASI* 06 (02): 76–81.

Putra, I Kadek Odie Kharisma, I Made Adi Darmawan, I Putu Gede Juliana, and Indriyani. 2022. "TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING." *CyberSecurity Dan Forensik Digital* 5 (2): 77–83.

Putra, Vikran Fasyadhiyaksa. 2021. "Modus Operandi Tindak Pidana Phising Menurut UU ITE." *Jurist-Diction* 4 (6): 2525–48. https://doi.org/10.20473/jd.v4i6.31857.

Putri, Adelia Khrisna, Axel Rizqy Saputra, Anna Nadia, and Febrina Yahya. 2023. "Building a Multi-Layered Support System for Students in Psychological Distress: Insights from Indonesian Faculty Members." *Psikologi* 50 (3): 259–82. https://doi.org/10.22146/jpsi.80921.

Widodo, Slamet, Festy Ladyani, La Ode Asrianto, Rusdi, and Khairunnisa. 2023. *BUKU AJAR METODE PENELITIAN*. PANGKALPINANG: CV Science Techno Direct.

Wijaya, Suparna, Ferry Irawan, Amrie Firmansyah, Jubaedah, Desmintari, and Praptiningsih. 2024. "INSTANSI PEMERINTAH SEBAGAI PENGUSAHA KENA PAJAK : PENGABDIAN KEPADA MASYARAKAT DALAM BENTUK VIDEO YOUTUBE Suparna." *PENGMASKU* 4 (1): 19–24.

Wiranata, Ganda Arisandi, Yoyok Ucuk, Subekti, and Dudik Djaja Sidarta. 2024. "PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING." *COURT REVIEW* 4 (02): 13–25.