Journal of Progressive Law and Legal Studies
E-ISSN 2986-9145 E-ISSN 3031-9242
Volume 3 Issue 03, September 2025, Pp. 331-347
DOI: https://doi.org/10.59653/jplls.v3i03.1858

Effectiveness of Legal Supervision by the Malang City Communication and Information Office on Phishing
(A Perspective of the ITE Law and Maqāṣid al-Sharīʿah)

Faishal Agil Al Munawar[1*], Maulida Zahro[2]
Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia[1]
Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia[2]
Corresponding Email: faishalagilalmunawar@uin-malang.ac.id*

Received: 04-06-2025 *Reviewed: 05-07-2025* *Accepted: 20-08-2025*

Abstract

Phishing refers to online fraud activities that deceive victims into disclosing their data, leading to various risks such as misuse of banking accounts, email accounts, and social media. This study is based on the increasing number of phishing cases in society, including among university students, which have resulted in financial losses and personal data breaches, thereby violating Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law). Therefore, local government supervision is deemed necessary to address phishing activities occurring in Malang City. The objective of this study is to analyze the effectiveness and challenges of the supervision carried out by the Department of Communication and Information (Diskominfo) of Malang City on phishing, from the perspective of the ITE Law and Maqāṣid al-Sharīʿah. The research employs an empirical juridical method with a socio-juridical approach. The findings indicate that the supervision efforts by Diskominfo Malang include public education on the dangers of phishing and prevention strategies, provision of a reporting channel called "Malangkota-CSIRT," and coordination with relevant stakeholders. From the perspective of Maqāṣid al-Sharīʿah, these efforts aim to realize public benefit (maslahah) by protecting wealth (hifzh al-mal) and life (hifzh al-nafs). However, the effectiveness of these supervision efforts remains limited due to legal constraints within the ITE Law and several practical challenges, such as unequal dissemination of information, limited human resources and budget, and inadequate infrastructure, all of which hinder the supervision and response process.

Keywords: Effectiveness; Phishing; Diskominfo; ITE Law; Maqāṣid al-Sharīʿah

Introduction

The development of information and communication technology in the digital era has transformed various aspects of human life, including the social, economic, and governmental sectors. Access to information has become faster and more open, and digital activities such as

online transactions and virtual communications are increasingly widespread among the public. However, this progress not only brings positive impacts but also opens up opportunities for increasingly complex cybercrimes. One of the most common and dangerous forms of cybercrime is phishing. Phishing is a fraudulent act carried out by impersonating a trusted party usually through electronic media such as emails, instant messages, or fake websites in order to steal personal data such as usernames, passwords, bank account information, and more. This crime is systematically committed by perpetrators who exploit system security vulnerabilities and the public's lack of digital literacy. Its impact extends beyond financial losses to victims; it also undermines data integrity and fosters insecurity in the use of digital services (Wibowo & Fatimah, 2017).

Malang City, as one of the major cities in Indonesia with a high rate of digitalization, is not immune to phishing threats. The high use of the internet, electronic transactions, and the presence of active academic and business communities contribute to the city's vulnerability to phishing attacks. According to data from the National Cyber and Crypto Agency (BSSN), hundreds of phishing cases are reported annually, including in Malang City where even government officials have fallen victim. This reality highlights the urgent need for serious preventive efforts and oversight from local authorities. The Malang City Government, through the Department of Communication and Information (Diskominfo), is actively involved in supervising and addressing cybercrimes, including phishing. Dr. Ir. Wahyu Hidayat, MM, as the Mayor of Malang, expressed his hope for the creation of a safe and conducive cyberspace in Malang, which would increase public trust and support economic growth in the city (Public Communication and Information Division, 2023).

The Department of Communication and Information (Diskominfo) of Malang City, as the institution authorized in the field of information and digital security, plays a crucial role in monitoring and addressing phishing cases. This role is stipulated in Malang Mayor Regulation Number 41 of 2021 concerning the Position, Organizational Structure, Duties, Functions, and Work Procedures of the Department of Communication and Information. Chapter IV, Article (2) letter j, states that one of the department's responsibilities is "the supervision and enforcement of regulations in the fields of communication, informatics, statistics, and cryptography."

Several efforts have been undertaken, including digital literacy education for the public, the provision of cyber incident reporting channels such as Malangkota-CSIRT, and collaboration with other government agencies. Nevertheless, these supervisory efforts still face various challenges, such as limited legal authority, a lack of competent human resources, restricted budgets, and inadequate infrastructure. The supervision of phishing crimes is based on Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), which is an amendment to the previous ITE Law. This law contains criminal provisions against perpetrators who illegally access data or information systems, as well as those who disseminate false information that harms consumers in electronic transactions. However, the effectiveness of this law remains a subject of debate, as its implementation at the regional level is often not supported by sufficient instruments and legal authority.

Effectiveness of Legal Supervision by the Malang City Communication and Information Office on Phishing

Article 28 paragraph (1) of the ITE Law states: "Any person who intentionally and without right disseminates false and misleading information resulting in consumer loss in electronic transactions." This aligns with Article 30 paragraphs (1) and (2), which stipulate: "(1) Any person who intentionally and without right or unlawfully accesses another person's computer and/or electronic system in any manner," and "(2) Any person who intentionally and without right or unlawfully accesses a computer and/or electronic system in any manner with the intent to obtain electronic information and/or electronic documents."

Data from the Ministry of Communication and Digital Affairs (Komdigi) in 2024 confirms the increasing threat of cybercrime. The National Cyber and Crypto Agency (BSSN) also reported handling 179 complaints submitted by regional communication and information offices, and the removal of 455 URLs containing elements of cybercrime, including phishing (Administrator, 2025). Based on interviews with staff from the Malang City Diskominfo, it was revealed that a head of a local government office in Malang was targeted in a phishing attack. The victim received a phishing message via WhatsApp, seemingly sent by their mobile provider, containing a link to a fake website. The total financial loss suffered amounted to IDR 600,000 (six hundred thousand rupiah) (Staff of the Malang City Communication and Information Office, personal communication, October 28, 2024). Thus, phishing is not merely a criminal issue but also has significant impacts on the economy and business. Moreover, victims are subjected to further harm, such as data breaches.

To address the threat of phishing, strategic measures are required. Strengthening digital security is crucial, including the regular updating of security software, the implementation of two-factor authentication, and public education to raise awareness of cyber threats (Curtis & Oxburgh, 2023). Cybercrime is a major challenge in the digital era that cannot be entirely avoided but can be mitigated through awareness and appropriate protective actions. Digital security is not only the responsibility of governments and corporations but also of every individual who uses technology (Dzaky & Edrisy, 2025). Therefore, building a secure and protected digital ecosystem has become an urgent necessity in an age where the virtual world is increasingly integrated into real life (Al-Khater et al., 2020).

However, the effectiveness of such supervision is not solely determined by the existence of regulations. As stated by Soerjono Soekanto in his theory of legal effectiveness, the implementation of a legal rule is influenced by five main factors: the legal substance, law enforcement agencies, facilities and infrastructure, the society, and the legal culture. In the context of Malang City, challenges such as the limited number of cybersecurity professionals, lack of technological infrastructure, and low levels of digital literacy among the public pose serious obstacles to the efforts to eradicate phishing. Therefore, a supervisory approach to phishing should not rely solely on repressive legal enforcement. Preventive and educational approaches that reach a broader public audience are also necessary. Public education, the provision of official reporting channels such as Malangkota-CSIRT, and cross-sectoral collaboration are key strategies employed by Diskominfo Malang. These efforts focus not only on responding to phishing attacks but also on fostering collective awareness of the importance of digital security (Brands & Van Doorn, 2022).

The Islamic legal approach through Maqāṣid al-Sharīʿah is also relevant in providing a strong value framework for the supervision of phishing crimes. Maqāṣid al-Sharīʿah refers to the essential objectives of Islamic law, which include the protection of religion (ḥifẓ al-dīn), life (ḥifẓ al-nafs), intellect (ḥifẓ al-'aql), lineage (ḥifẓ al-nasl), and wealth (ḥifẓ al-māl). In this context, phishing is a form of crime that undermines the values of protecting life and wealth, as it causes material loss and psychological distress to victims. Therefore, this approach is important in developing a supervisory system that is not only legal-formal in nature but also ethical and beneficial (maslahah)-oriented. As a foundational principle of Islamic law, Maqāṣid al-Sharīʿah offers an approach focused on the protection of wealth (ḥifẓ al-māl) and life (ḥifẓ al-nafs), which is highly relevant in formulating legal oversight policies that aim not only to punish perpetrators but also to prevent broader societal harm.

This study is intended to complement previous research on the effectiveness of oversight and handling measures taken by Diskominfo Malang City in combating phishing, viewed from the perspective of the ITE Law and Maqāṣid al-Sharīʿah. It seeks to provide a comprehensive picture of how local governments play a role in protecting society from digital crimes. The study is expected to contribute to the formulation of more integrative and responsive policies that address the challenges of the digital era, both in terms of national legal frameworks and the values of Islamic law. Accordingly, this research will address the following issues: (a) the effectiveness of Diskominfo Malang's supervision of phishing from the perspective of the ITE Law and Maqāṣid al-Sharīʿah; and (b) the obstacles faced by Diskominfo Malang in carrying out this supervision.

Literature Review

Effectiveness

Etymologically, the word "effectiveness" originates from the English word effective, which means successful. According to the Indonesian Dictionary (Kamus Besar Bahasa Indonesia or KBBI), effectiveness refers to a condition or quality of having influence, being efficacious, successful, and capable of producing the desired outcomes, or the ability of an action to achieve predetermined objectives. Legal and socio-legal scholars interpret the meaning of legal effectiveness in various ways, depending on their respective perspectives (Orlando, 2022). According to Soerjono Soekanto, legal effectiveness refers to legal norms that serve as a standard for appropriate attitudes, actions, or behaviors. It can typically be assessed by determining whether the law successfully influences certain behaviors in accordance with its intended purpose. Soekanto also argues that the effectiveness of law can be measured by the extent to which a group or society is able to achieve its goals (Soekanto, 1988).

According to Barnard, effectiveness refers to the dynamic condition of a series of processes in carrying out tasks and functions in accordance with the objectives and policy instruments of an established program. Based on this conceptual definition, one key dimension of analysis is the effectiveness of the program itself (Rahayu et al., 2021). Understandings of effectiveness as proposed by various scholars may vary depending on each individual's academic background. However, these interpretations generally converge on a common goal:

achieving the desired outcomes. In this study, effectiveness refers to the achievements and objectives, as well as the role of the local government agency namely the Department of Communication and Informatics (Diskominfo) of Malang City in overseeing digital crimes such as phishing. The measures and actions taken by the institution are assessed based on their success in achieving compliance with applicable laws and regulations.

Supervision

Supervision can be interpreted as “ensuring or guaranteeing” that organizational and managerial objectives are achieved. It serves as a means to ensure that activities are carried out in accordance with the planned objectives. According to the *Kamus Besar Bahasa Indonesia* (KBBI), the term *pengawasan* (supervision) means "monitoring and safeguarding." Meanwhile, the *Legal Dictionary* defines supervision as "the alignment between plans and actual achievements" (Jayanti, 2022).

The definition of regional government supervision, based on Article 1 paragraph (3) of the Regulation of the Minister of Home Affairs of the Republic of Indonesia Number 19 of 2024 concerning the Planning, Development, and Supervision of Regional Government Administration in 2024, states that supervision is an effort, action, and activity aimed at ensuring that the implementation of local governance is conducted efficiently and effectively in accordance with the applicable laws and regulations. Furthermore, Article 33 paragraph (2) of Government Regulation Number 82 of 2012 on the Implementation of Electronic Systems and Transactions specifies that supervision includes monitoring, controlling, auditing, tracing, and securing activities.

According to Robert J. Mockler, supervision is "a structured or systematic effort that involves the establishment of performance standards, the generation of feedback systems, comparing actual activities with predetermined standards, identifying and measuring deviations, and taking corrective actions to ensure the most efficient and effective use of all organizational resources in achieving business objectives" (Mufallihah, 2022). Another opinion is expressed by Hendyat Soetopo, who defines supervision as an activity aimed at controlling, evaluating, and developing actions to align with the previously established plans and objectives. Therefore, supervision serves as a benchmark for determining what should be achieved in alignment with the overall plan (Tadjudin, 2013).

Phising

Phishing is a type of cybercrime committed to steal personal information by impersonating an official entity or institution in order to obtain sensitive data such as passwords, credit card numbers, and email addresses registered with banking accounts. Phishing can be carried out through emails, text messages, phone calls, or malicious links. The primary aim of phishing is to deceive individuals into voluntarily and unknowingly disclosing their personal information. This type of crime results in financial losses and undermines public trust in electronic transactions and related institutions. Consequently, it can have a broader negative impact on economic growth (Hanifah, 2023).

ITE Law

The Electronic Information and Transactions Law, commonly abbreviated as the ITE Law, is one of the regulations in Indonesia that governs electronic information and transactions, including information technology in general. This law regulates the use of information technology, including the rights and obligations of internet users, the protection of personal data, and criminal acts related to the misuse of information technology. The ITE Law has undergone several amendments. Law Number 11 of 2008 was the first version enacted, followed by the first amendment in 2016, and the second amendment in 2024. Cybercrimes can also be prosecuted under the provisions of this law, as such acts may violate several articles contained within it (Administrator, 2025).

Maqāṣid al-Sharīʿah

Linguistically, Maqāṣid al-Sharīʿah consists of two words: Maqāṣid, meaning "intentions" or "purposes," and al-Sharīʿah, meaning "the path" or "the straight way." Terminologically, Maqāṣid al-Sharīʿah refers to the ultimate objectives of Islamic law as ordained by Allah, aiming to preserve human welfare (maslahah) and protect against harm (mafsadah), both in this world and in the hereafter. The classical theory of Maqāṣid al-Sharīʿah outlines five essential objectives that form the foundation of Islamic legal and ethical reasoning. These are: Hifz al-Din (protection of religion), which ensures the preservation and freedom of religious belief and practice; Hifz al-Nafs (protection of life), which upholds the sanctity and security of human life; Hifz al-Mal (protection of property), which safeguards individual ownership and financial rights; Hifz al-'Aql (protection of intellect), which emphasizes the importance of knowledge, education, and sound reasoning; and Hifz al-Nasl (protection of lineage), which ensures the integrity of family structure and the moral upbringing of future generations. These five dimensions reflect the comprehensive vision of Islam in promoting justice, balance, and the holistic development of human life (Jalili, 2021).

Research Method

This study employs empirical legal research, which conceptualizes law as actual behavior, grounded in empirical facts obtained from the field. The approach used is the socio-juridical approach, which examines how law operates within society and the extent to which legal norms are applied in practice (Muhaimin, 2015). This approach is essential because it views law not merely as a normative text but as a component of social practice involving interactions among government institutions, the public, and the legal norms themselves. The types of data used in this research include primary data obtained directly through interviews with staff and officials of the Department of Communication and Information (Diskominfo), as well as secondary data consisting of documents, statutory regulations such as Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law) and relevant literature related to the research topic. Data collection techniques include in-depth interviews, documentation, and literature review (Abdulkadir, 2004; Ibrahim, 2008).

Effectiveness of Legal Supervision by the Malang City Communication and Information Office on Phishing

The collected data were analyzed qualitatively using descriptive-analytical techniques, which involve describing field conditions and analyzing them in light of relevant theories and legal provisions (Nur, 2019). This study applies Soerjono Soekanto's theory of legal effectiveness as its main analytical framework, which assesses legal effectiveness based on five factors: the legal substance itself, law enforcement officials, supporting facilities and infrastructure, the society, and legal culture. In addition, the principle of Maqāṣid al-Sharīʿah is employed to evaluate the extent to which Diskominfo's supervision aligns with the Islamic values of protecting wealth (ḥifẓ al-māl) and life (ḥifẓ al-nafs).

Result and Discussion

Evaluating the Effectiveness of Diskominfo Malang's Oversight of Phishing: An Analysis Based on the ITE Law and Maqāṣid al-Sharīʿah Perspective

Based on previous findings by Andre Aditya Iman (2023) in a journal article titled "Legal Review of Cyber Phishing Crimes Committed to Steal Personal Data on Digital Trading Platforms in Relation to Law Number 19 of 2016 Concerning the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions", a significant gap was identified namely the lack of oversight by government institutions regarding phishing activities (Ferrary et al., 2023). The earlier study focused primarily on phishing cases involving the theft of personal data on digital trading websites. Therefore, this current article shifts focus to evaluating the effectiveness of supervision carried out by the Malang City Department of Communication and Information (Diskominfo) from the perspective of Maqāṣid al-Sharīʿah.

This research also aims to fill a gap in the existing literature, which has seldom addressed the local government's role in supervising phishing crimes, particularly in Malang City. Most prior studies have concentrated on national regulatory frameworks or normative case analyses. Through this study, it is expected that a more comprehensive understanding of local oversight mechanisms in combating phishing crimes can be achieved, and that such understanding may contribute to improving effectiveness through enhanced regulations, institutional capacity building, and public education.

The supervision carried out by the Malang City Department of Communication and Information (Diskominfo) on phishing as a form of cybercrime is a critical step in addressing the increasing prevalence of cyber threats in the digital era. Phishing, as a digital crime, exploits psychological manipulation to acquire personal data such as banking information, email credentials, and social media accounts. This phenomenon causes not only financial loss but also diminishes public trust in digital systems. Diskominfo Malang acts as the front-liner in providing education, reporting mechanisms, and initial facilitation for phishing victims. Within Diskominfo Malang, cybercrime-related matters, including phishing, are primarily handled by the Statistics and Cryptography Division, with support from the Application and Informatics Division (Aptika) in carrying out related tasks. The oversight implemented by Diskominfo Malang is indirect in nature and largely preventive. Such local government supervision serves as a measure of legal effectiveness in achieving predetermined legal objectives.

According to cybercrime reports obtained from the Malang City Department of Communication and Information (Diskominfo), particularly concerning phishing from 2023 to 2024 (as of December), a total of 144 reports were received. However, these reports were grouped together with XSS (Cross-Site Scripting) attacks, as both involve deceiving victims through malicious links with the aim of obtaining personal data (Karina Ayu Dewanti, personal communication, April 14, 2025). Handling of cyberattack reports, including phishing, is the responsibility of the Statistics and Cryptography Division. This division receives the reports and forwards them to the National Cyber and Crypto Agency (BSSN). Once access is granted, the matter is handed over to the Application and Informatics Division (Aptika) to be blocked through the city's cybersecurity systems.

From the perspective of Law Number 1 of 2024 on Electronic Information and Transactions (ITE Law), this form of supervision aligns with Article 28 and Article 30, which prohibit the dissemination of misleading information and unauthorized access to electronic systems. Diskominfo functions as a liaison between the public and law enforcement agencies by providing a reporting channel through Malangkota-CSIRT (Computer Security Incident Response Team). This platform allows the public to directly report cyber incidents, including phishing. Malangkota-CSIRT was officially established in November 2023 with the aim of preventing, mitigating, and responding to cybersecurity incidents, including phishing attacks (Administrator, 2023).

Diskominfo also engages in public education through outreach activities, digital security campaigns, and public warnings about the latest phishing tactics. However, in practice, the effectiveness of these supervisory efforts remains suboptimal due to the limited authority of Diskominfo, which functions as an administrative body rather than a law enforcement agency. As a result, most of the measures taken are preventive and informative in nature rather than repressive. Additional challenges include unequal distribution of skilled human resources, limited budgets, and insufficient technological infrastructure, all of which reduce the overall effectiveness of the supervision. Many areas in Malang City have not yet received adequate outreach, especially among laypeople and students, resulting in low digital literacy and a higher risk of phishing victimization. Diskominfo also faces technical barriers such as inadequate cybersecurity infrastructure, insufficient funding, and a lack of qualified personnel in the field of digital security. These issues directly affect the scope and effectiveness of oversight efforts. Many residents remain unaware of the importance of digital security due to a lack of sufficient public education.

In response, Diskominfo Malang has taken steps to strengthen its infrastructure by enhancing cybersecurity measures in collaboration with relevant stakeholders. Notably, Diskominfo has partnered with Telkomsigma to monitor servers and implement Endpoint Detection and Response (EDR) systems. EDR is a cybersecurity solution designed to detect and respond to cyber threats at endpoint devices such as computers, laptops, and servers. It is capable of identifying both known and unknown threats in real time and preventing the spread of attacks (Kaur et al., 2024).

From the perspective of implementation, the effectiveness of supervision still encounters numerous obstacles. One of the main challenges lies in the limited legal authority

granted to Diskominfo. As a regional government agency, Diskominfo does not possess the jurisdiction to conduct investigations or take direct legal action against perpetrators of phishing. Its supervisory function is confined to reporting incidents and coordinating with law enforcement authorities. This limitation poses a significant barrier to following up on cases swiftly and effectively. Inter-agency collaboration emerges as a crucial solution to enhance effectiveness. Diskominfo must strengthen its synergy with the police, the National Cyber and Crypto Agency (BSSN), and religious institutions to establish a more comprehensive legal and spiritual approach. Preventive measures must also be complemented by firm legal actions against cybercriminals to create a deterrent effect and to increase the public's sense of security.

According to Soerjono Soekanto, legal effectiveness refers to the extent to which a group is able to achieve the goals that have been set. Law is considered effective when all relevant actors, including the government and society, behave in accordance with legal norms and provisions (Soekanto, 1988). Based on Soekanto's theory of legal effectiveness, there are five factors used to assess whether the law functions properly (Soekanto, 2016):

1. Legal Substances (Factor of Law Itself)

This factor refers to the content of the law, which functions to regulate various aspects of societal life in an orderly and just manner. Soekanto points out that in practice, the application of laws often encounters several problems, such as: First, the failure to apply the principles governing the applicability of legislation. Second, the absence of necessary implementing regulations that ensure the law is effectively operational. Third, ambiguity in the wording of legal provisions, which leads to confusion in interpretation and implementation. In carrying out its duties and functions, the Department of Communication and Informatics (Diskominfo) of Malang City has aligned its actions with Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE Law) and Mayor Regulation No. 42 of 2021.

2. Law Enforcement Apparatus

Soekanto explains that every law enforcer holds a specific status and role within the social structure, encompassing inherent rights and obligations. These responsibilities shape the roles they must perform. According to Article 43 Paragraphs (1) and (2) of Law No. 1 of 2024 on Electronic Information and Transactions, Civil Servants (PNS) in government institutions whose duties relate to information technology and electronic transactions are granted specific authority to act as investigators. This authority must be exercised while upholding privacy, confidentiality, the smooth delivery of public services, and data integrity, in accordance with relevant laws and regulations. In this context, Diskominfo of Malang City acts as an administrative enforcement body engaged in indirect legal supervision.

3. Facilities and Infrastructure

Infrastructure and facilities play a pivotal role in supporting the effectiveness of legal enforcement. Without sufficient infrastructure, implementation will face substantial obstacles, making it difficult to achieve optimal results. The availability of adequate infrastructure enables the law to function more efficiently. Diskominfo Malang has taken steps to strengthen its cybersecurity infrastructure through collaborations with various stakeholders such as

Telkomsigma, the Ministry of Communication and Informatics, the National Cyber and Crypto Agency (BSSN), the Indonesian National Police, and the Malang City Government. However, the agency still faces challenges such as budget limitations, which lead to shortages in skilled human resources and technological infrastructure. These constraints negatively affect the agency's response time in handling cyberattacks.

4. Society

A well-ordered and regulated society is supported by a governing structure that is human-made to manage its own life. In this case, that structure is law, which functions as a guideline for ensuring order and harmony (Nur, 2019). The participation of the public in supporting Diskominfo's role is crucial in creating a secure digital environment. It is essential for communities to be involved in promoting awareness of the dangers of cybercrime. The synergy between society and government support will generate long-term, positive impacts. Although the Department of Communication and Informatics (Diskominfo) of Malang City has actively conducted public education through social media campaigns and direct outreach programs, public legal awareness remains low. Many citizens are still unaware of the existence of the Computer Security Incident Response Team (CSIRT) or the appropriate procedures for reporting phishing attempts. This lack of digital literacy poses a significant barrier to the effectiveness of law within society. Therefore, collaborative efforts with the community are essential to enhance digital literacy, reduce potential losses, and prevent the erosion of public trust in financial institutions. The public plays a vital role in ensuring legal effectiveness, as they are directly involved and are the primary subjects required to comply with the established regulations.

5. Legal Culture Factor

According to Soerjono Soekanto, culture plays a vital role in the life of society. Its primary function is to guide individuals in understanding how to act, behave, and determine appropriate attitudes when interacting with others. Thus, culture is not merely a set of traditions, but rather a collection of values and norms that direct human behavior by defining what is permissible and what must be avoided. In the context of digital crimes such as phishing, many internet users are still easily deceived by fraudulent schemes, such as fake links embedded in websites that lead to phishing attacks. This indicates that a digital legal culture has not yet been firmly established. Therefore, it is necessary for both local governments and the community to actively work together to create a safe and ethical digital environment.

Based on the five aforementioned factors regarding the effectiveness of legal supervision by the Malang City Department of Communication and Information (Diskominfo) from the perspective of Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), it can be seen that there are both strong and weak aspects. This indicates an imbalance and a lack of integration among the factors, which ultimately results in less-than-optimal legal effectiveness (Soekanto, 2016).

Law is considered effective when all parties, including the government and society, behave in accordance with legal provisions. The success of legal implementation is reflected when its enforcement yields a positive impact on society, as evidenced by the achievement of

its goals in guiding or transforming public behavior to align with existing legal norms. However, if the legal provisions are only partially implemented or not applied comprehensively, the intended objectives of the law will not be optimally or effectively realized.

From the perspective of Maqāṣid al-Sharīʿah, the supervision carried out by the Malang City Department of Communication and Informatics (Diskominfo) reflects two primary principles: ḥifẓ al-māl (protection of wealth) and ḥifẓ al-nafs (protection of life). Preventive actions such as public education and reporting mechanisms are efforts to protect the public from financial losses and psychological trauma caused by phishing attacks. In this regard, Diskominfo performs a socio-religious function aimed at promoting public welfare (maṣlaḥah) and preventing harm (mafsadah).

According to ʿAbd al-Majīd al-Najjār, the objectives of Islamic law (maqāṣid al-sharīʿah) should encompass eight essential necessities (al-ḍarūriyyāt al-thamāniyyah): ḥifẓ al-dīn (protection of religion), ḥifẓ insāniyyah al-insān (preservation of human dignity), ḥifẓ al-nafs al-insāniyyah (protection of human life), ḥifẓ al-‘aql (preservation of intellect), ḥifẓ al-nasl (protection of progeny), ḥifẓ al-kiyān al-ijtimāʿī (protection of social order), ḥifẓ al-māl (protection of wealth), and ḥifẓ al-bīʾah (protection of the environment). The ultimate goal of the Sharīʿah is to ensure human welfare in this world and the Hereafter, by bringing about benefit and preventing harm (Al Munawar, 2021). However, maqāṣid al-sharīʿah also emphasize the importance of sustainability and effectiveness in achieving such protections. Thus, if current efforts remain temporary and fail to address root issues such as the lack of binding legal frameworks or insufficient technological readiness then the objectives of the maqāṣid have not yet been fully realized. In this context, a more comprehensive and sustainable policy reform is necessary (Iqbal, 2019).

The connection between Diskominfo’s role and the maqāṣid al-sharīʿah lies in the ultimate aim of safeguarding human wealth. From this perspective, the actions taken by Diskominfo should result in maṣlaḥah (public benefit) that aligns with the essential needs of human life. At its core, the wisdom behind ḥifẓ al-māl (protection of wealth) and ḥifẓ al-nafs (protection of life) is to ensure that individuals acquire wealth through lawful means and that their lives are safeguarded, as Islam strictly prohibits the consumption of wealth obtained through illegitimate or deceptive practices. In doing so, society can achieve a higher standard of well-being and justice.

In summary, Diskominfo’s supervision of phishing in Malang City is aligned with both positive law and the values of maqāṣid al-sharīʿah, but remains limited in scope and impact. Strengthening legal frameworks, improving digital literacy, and integrating Islamic ethical values into public policy are all essential steps. With these improvements, the effectiveness of oversight can be significantly enhanced, ensuring better protection for Malang City residents in the digital era.

Obstacles Encountered by the Malang City Communication and Informatics Office in Addressing Phishing Threats

In carrying out its supervisory duties related to phishing cybercrimes, the Department of Communication and Information Technology (Diskominfo) of Malang City encounters several challenges that directly affect the effectiveness of its efforts. The most fundamental barrier is the limitation of legal authority. As an administrative agency, Diskominfo does not possess the legal mandate to conduct investigations, prosecutions, or legal proceedings against phishing perpetrators. Such authority lies exclusively with law enforcement agencies such as the police or the National Cyber and Crypto Agency (BSSN). Consequently, Diskominfo's role is restricted to preventive and coordinative actions, such as public education and reporting, without the capacity to take direct legal action against offenders. Budget constraints also significantly impact the technological infrastructure. Central government budget efficiency policies have led to suboptimal operational performance within Diskominfo. Implementing broader educational and awareness programs requires substantial funding (Ramlan & Riza, 2024). These limitations in infrastructure and budget hinder effective supervision, resulting in prolonged response times in handling phishing incidents.

The second major barrier is the shortage of qualified human resources, particularly in the field of cybersecurity (Fatmawati & Sesung, 2024). There is a notable lack of skilled technical personnel, especially penetration testers (pentesters), whose role involves simulating cyberattacks to identify system vulnerabilities (Singasatia, 2006). The recruitment of such professionals is difficult due to the need for specialized training and certification, which entails a long and rigorous process (Karina Ayu Dewanti, personal communication, April 23, 2025). This limitation affects Diskominfo's ability to conduct early detection and attack simulations. Although Diskominfo has established a Computer Security Incident Response Team (CSIRT), its personnel and expertise remain inadequate to anticipate and address the increasingly complex and rapidly evolving phishing threats. Moreover, regular staff training has not been maximized due to the absence of sustainable capacity-building programs.

The third obstacle lies in the lack of advanced technological infrastructure and supporting systems. Combating sophisticated cybercrimes requires up-to-date software and hardware, as well as a reliable communication network. Diskominfo Malang continues to face limitations in digital tracking systems, integrated data centers, and early warning mechanisms for phishing threats (Nurmala et al., 2023). These deficiencies hinder prompt identification and mitigation, as well as the effective handling of public reports. Additionally, funding for cybersecurity initiatives remains minimal. Digital monitoring programs such as literacy campaigns, HR capacity development, and the procurement of security technologies still rely heavily on regional budget allocations (APBD), which often do not prioritize this sector. Meanwhile, phishing crimes continue to evolve and require regular updates to tools and technology. Without adequate financial support, Diskominfo cannot ensure equitable and widespread public outreach.

Another significant challenge is the low level of digital literacy among the public, particularly among students, the elderly, and those with limited access to technology. Many

citizens cannot distinguish between legitimate and fake websites and are unaware of the risks associated with clicking suspicious links. This issue is exacerbated by the rapid spread of hoaxes and false information on social media, making it easier for phishing actors to exploit public ignorance. Diskominfo faces substantial difficulties in transforming digital behavior and mindsets that are deeply ingrained, indicating that a strong culture of digital legal awareness and literacy has yet to be fully established.

Coordination among institutions, both at local and national levels, also remains a major hurdle. Although a reporting mechanism through Malangkota-CSIRT exists, follow-up processes are often delayed due to limited coordination with the police, BSSN, and financial institutions. The lack of integration in reporting and enforcement systems hampers effective phishing management, complicating documentation, investigation, and prevention efforts. From a regulatory standpoint, there is a mismatch between the need for digital protection and existing legal provisions, particularly within the Electronic Information and Transactions Law (UU ITE). While the law prohibits the dissemination of false information and illegal access to electronic systems, its implementing regulations do not fully delineate the responsibilities of regional governments in terms of prevention, education, and victim recovery. This regulatory gap renders Diskominfo's role vulnerable to stagnation and lacking normative support for long-term strategic actions.

In general, these barriers are interrelated and demonstrate that effective phishing oversight requires an integrated, cross-sectoral approach. A synergistic framework is needed combining clear legal regulations, adequate funding, qualified human resources, robust infrastructure, and active community participation. Without strengthening these key aspects, Diskominfo Malang's efforts will remain limited to informative functions and fall short in addressing the growing complexity of phishing crimes.

In response to the escalating threat of phishing cybercrimes, Diskominfo Malang has implemented several strategic initiatives. The most prominent is the establishment and management of the Malangkota-CSIRT (Computer Security Incident Response Team), a formal channel for public reporting of digital crimes, including phishing. This unit coordinates with relevant institutions such as the police and BSSN to follow up on reports. It plays a vital role as a bridge between victims and law enforcement.

Additionally, Diskominfo Malang actively engages in digital literacy and education campaigns, utilizing social media, seminars, and direct outreach to schools and community groups. The primary objective of these initiatives is to raise public awareness about the forms of phishing, common attack methods, and preventive measures. This educational approach is crucial because phishing attacks often succeed due to victims' lack of awareness and insufficient digital security knowledge.

Another initiative includes institutional collaboration, both vertically with national ministries and agencies and horizontally with regional institutions such as police departments, prosecutors, and educational entities. Such partnerships enable an integrated response to phishing from detection and reporting to verification and public dissemination of threat

information. This collaboration ensures that phishing cases can be addressed more swiftly and accurately.

Diskominfo also contributes by formulating internal and technical cybersecurity policies, such as designing monitoring systems for suspicious digital activities and conducting rapid reporting to national cybersecurity control centers. While Diskominfo lacks legal enforcement authority, its role in early detection and initial mitigation is crucial to prevent the wider impact of phishing attacks.

Nevertheless, despite these various efforts, challenges persist. The success of these initiatives heavily depends on public participation and understanding of the importance of personal information security. On the other hand, Diskominfo continues to require strengthening in terms of budget, technology, and regulatory support to enable a more effective and comprehensive supervisory function.

In conclusion, while Diskominfo Malang has taken appropriate preventive and collaborative measures in addressing phishing crimes, these efforts have not yet reached optimal effectiveness. Enhancing the legal framework, institutional capacity, and multisectoral synergy is essential to ensure that phishing crime management is systematic, swift, and capable of addressing the root causes of the issue.

Conclusion

Based on the aforementioned analysis, the following conclusions can be drawn regarding "The Effectiveness of Legal Supervision by the Malang City Communication and Information Office on Phishing: A Perspective of the ITE Law and Maqāṣid al-Sharīʿah": First, Diskominfo Malang has taken preventive measures such as public education, providing a reporting channel (MalangKota-CSIRT), and implementing system-based blocking mechanisms through digital security infrastructure. However, referring to Soerjono Soekanto's five legal effectiveness factors, the supervision carried out by Diskominfo Malang is considered less effective due to the presence of both weak and strong elements among these factors, which hinders the overall performance and completeness of its implementation. From the perspective of Maqāṣid al-Sharīʿah, the supervision conducted by Diskominfo aligns with the objective of protecting wealth (hifz al-mal) by aiming to prevent financial losses suffered by the public as a result of phishing activities. Phishing, which involves unauthorized acquisition of someone's property, is fundamentally prohibited in Islamic law, as it constitutes a form of unjust seizure of ownership rights.

Second, the main barriers to achieving effective supervision by Diskominfo Malang in addressing cybercrimes such as phishing include: the public's lack of awareness regarding the existence and function of the "MalangKota-CSIRT" reporting channel; a shortage of skilled human resources in the cybersecurity field; and limited infrastructure and budget, all of which significantly impede effective handling and oversight of phishing cases. Nevertheless, Diskominfo Malang has undertaken mitigation efforts to address these challenges by strengthening coordination with relevant stakeholders and conducting socialization and

educational programs targeted at both the general public and local government institutions across the city. These efforts aim to foster digital awareness, improve reporting engagement, and enhance the region's overall cybersecurity resilience.

References

Abdulkadir, M. (2004). *Hukum dan penelitian hukum*. Bandung: Citra Aditya Bakti.

Administrator. (2023, November 8). *Malang City launches CSRIT*. East Java Communication and Information Office. Retrieved May 5, 2025, from https://kominfo.jatimprov.go.id/index.php/berita/kota-malang-luncurkan-csirt

Administrator. (2023). *Main duties and functions*. Malang City Communication and Information Office. Retrieved April 30, 2025, from https://kominfo.malangkota.go.id/

Administrator. (2025, February 26). *Social cyber threats are increasing, Head of Kominfo urges enhanced digital security awareness*. East Java Communication and Information Office. Retrieved May 1, 2025, from https://kominfo.jatimprov.go.id/berita/ancaman-siber-sosial-meningkat-kadis-kominfo-harap-kesadaran-keamanan-digital-ditingkatkan

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access, 8*. https://doi.org/10.1109/ACCESS.2020.3011259

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. In *Computers in Human Behavior* (Vol. 127). https://doi.org/10.1016/j.chb.2021.107082

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *Police Journal*, *96*(4). https://doi.org/10.1177/0032258X221107584

Fatmawati, I., & Sesung, R. (2024). Issuance of Building Approval (PBG) for Development on Land Affected by Street Plans in Surabaya City. *Journal of Progressive Law and Legal Studies*, *2*(03 SE-Articles), 210–224. https://doi.org/10.59653/jplls.v2i03.1062

Ferrary, A. A. I., Hartini, S., & Purwaningsih, P. (2023). Kajian hukum terhadap tindak pidana cyber phishing yang digunakan untuk mengambil data pribadi pada situs digital trading. *Yustisi*, *10*(2), 1–12. https://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/view/14314

Government of Indonesia. (2024). *Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law)*. Jakarta: State Secretariat of the Republic of Indonesia.

Hanifah, Lutfiyatul. (2023). *Pengaturan tindak pidana cyber crime dalam bentuk cyber phishing menurut hukum pidana Indonesia*. Undergraduate thesis, Universitas Islam Sultan Agung Semarang. http://repository.unissula.ac.id/30148/

Hasanuddin, W. F., & Imran. (2020). *Pengawasan hakim dan penegakan kode etik di Komisi Yudisial*. Jakarta: Sinar Grafika.

Ibrahim, J. (2008). *Teori dan metodologi penelitian hukum normatif*. Surabaya: Bayumedia.

Iqbal, M. (2019). MAQASID SYARIAH SEBAGAI DASAR PARADIGMA EKONOMI ISLAM. *Hikmah*, *16*(2), 47–58. Retrieved from https://e-jurnal.staisumatera-medan.ac.id/index.php/hikmah/article/view/46

Jayanti, N. (2022). Mekanisme pengawasan terhadap produk hukum dalam konstruksi politik hukum. *Jurnal Ilmu Hukum Tambun Bungai*, *7*(2), 176–192. http://dx.doi.org/10.61394/jihtb.v4i2.84

Jalili, A. (2021). The theory of Maqashid Sharia in Islamic law. *Teraju: Jurnal Syariah dan Hukum*, *3*(2), 71–80. https://doi.org/10.35961/teraju.v3i02.294

Kaur, H., Sanjaiy, D., Paul, T., Thakur, R. K., Kumar, K. V., Jay, R., & Naveen, M. K. (2024). Evolution of endpoint detection and response (EDR) in cyber security: A comprehensive review. *E3S Web of Conferences, 556*. https://doi.org/10.1051/e3sconf/202455601006

Mayor of Malang City. (2021). *Mayor Regulation Number 41 of 2021 on the Position, Organizational Structure, Duties and Functions, and Working Procedures of the Department of Communication and Informatics of Malang City*. Malang City Government.

Mufallihah, Mailadatul. (2021). *Pengawasan Otoritas Jasa Keuangan terhadap layanan pinjaman online berbadan koperasi yang belum berizin di Otoritas Jasa Keuangan*. Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim. http://etheses.uin-malang.ac.id/30995/

Muhaimin. (2015). *Metode penelitian hukum*.

Muhammad Aabid Tyas Dzaky, & Ibrahim Fikma Edrisy. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *4*(2), 3614–3625. https://doi.org/10.56799/peshum.v4i2.8311

Al Munawar, F.A. (2021). 'Abd al-Majīd al-Najjār's Perspective on Maqāṣid al-Sharī'ah. *JURIS (Jurnal Ilmiah Syariah)*, *20*(2), pp.209-223. http://dx.doi.org/10.31958/juris.v20i2.4281

Nur, S. (2021). *Buku pengantar penelitian hukum*.

Nur, S. (2019). *Masyarakat dan penegakan hukum*. Pasuruan: Qiara Media.

Nurmala, L., Kodai, D. A., & Ahmad, I. (2023). Supervision and Law Enforcement Efforts on Food Products Unfit for Consumption Based on Law Number 18 of 2012 concerning Food. *Journal of Progressive Law and Legal Studies*, *1*(03), 187–196. https://doi.org/10.59653/jplls.v1i03.312

Orlando, G. (2022). Efektivitas hukum dan fungsi hukum di Indonesia. *Jurnal Pendidikan Agama dan Sains*, *6*, 50–58. https://doi.org/10.58822/tbq.v6i1.77

Public Communication and Information Division. (2023, November 8). *As a form of cyber protection commitment, Malang City Government launches MalangKota-CSRIT*. Malang City Government. Retrieved March 12, 2025, from https://malangkota.go.id/2023/11/08/wujud-komitmen-perlindungan-siber-pemkot-malang-luncurkan-malangkota-csirt/

Ramlan, R., & Riza, F. (2024). Supervision of Fishery Resources through Integrated Technology. *Journal of Progressive Law and Legal Studies*, *2*(02), 82–92. https://doi.org/10.59653/jplls.v2i02.646

Sururama, R., & Amalia, R. (2020). *Pengawasan pemerintah*. Jatinangor: Cendekia Press.

Singasatia, S., et al. (2006). Penetration testing untuk menguji kerentanan pada sistem informasi akademik di Sekolah Tinggi Teknologi XYZ. *Sekolah Tinggi Teknologi Wastukancana.*

Tadjudin, T. (2013). Supervision in educational management. *Ta'allum: Jurnal Pendidikan Islam, 1*(2). *https://doi.org/10.21274/taalum.2013.1.2.195-204*

Soekanto, S. (1988). *Efektivitas hukum dan penerapan sanksi*. Bandung: Ramadja Karya.

Soekanto, S. (2016). *Faktor-faktor yang mempengaruhi penegakan hukum*.

Sudaryono. (2016). *Metode penelitian pendidikan*. Jakarta: Kencana.

Suyanto. (n.d.). *Metode penelitian: Hukum pengantar normatif, empiris, dan gabungan*.

Wibowo, M. H., & Fatimah, N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JoEICT (Journal of Education and ICT), 1(1), 1–5. https://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69*