ISRG Journal of Arts, Humanities and Social Sciences (ISRGJAHSS)

ISRG PUBLISHERS
Abbreviated Key Title: ISRG J Arts Humanit Soc Sci
ISSN: 2583-7672 (Online)
Journal homepage: https://isrgpublishers.com/isrgjahss
Volume – III Issue –IV (July-August) 2025
Frequency: Bimonthly

Countermeasures Against Cyber Phishing Crimes Under the Electronic Information and Transactions Law

Farid Al Fauzi[1*], Setiyono[2], Kadek Wiwik Indrayanti[3]

[1, 2, 3] Master of Law, University Merdeka Malang

| **Received:** 31.07.2025 | **Accepted:** 05.08.2025 | **Published:** 07.08.2025

***Corresponding author:** Farid Al Fauzi
Master of Law, University Merdeka Malang

Abstract

This study analyzes handling cyber phishing crimes in the jurisdiction of the Malang City Police based on the Electronic Information and Transactions Law (ITE). The sociological juridical method with an empirical approach is used through interviews and direct observation. The results show that the success of handling cyber phishing is greatly influenced by the competence of personnel and the availability of adequate technological equipment, such as digital forensic devices and network monitoring systems. The main obstacles include limited expert personnel, inadequate technological facilities, and low public awareness. The Malang City Police optimizes resources to handle cases, cooperate between agencies, and improve the public reporting system. The study emphasizes the importance of synergy between institutions, personnel competency training, technology modernization, and public education to increase the effectiveness of handling cyber phishing. These findings support the theory of legal effectiveness, which emphasizes the role of professional officers and a good legal culture in changing public behavior according to legal norms.

Keywords: *Cyber Phishing, Law Enforcement, Cyber Crime*

INTRODUCTION

The rapid advancement of information and communication technology has significantly impacted various aspects of human life. Computers and the internet have become integral to daily activities, ranging from communication and business transactions to public services. However, this technological progress has also created opportunities for the emergence of increasingly complex forms of cybercrime that harm society. One particularly prevalent and concerning type of cybercrime is cyber phishing, an online fraud technique aimed at obtaining sensitive information such as user IDs, passwords, and other personal data by deceiving victims through emails, fake websites, text messages, or chat applications.

DOI: 10.5281/zenodo.16757823

One of the manifestations of advancements in information technology today is the use of computers in telecommunications and information delivery. A computer is an electronic system capable of receiving, processing, storing, and producing data or information based on given instructions. The main components of a computer include hardware, software, operational procedures, users or human resources (brainware), and the content in the form of data or information itself. These components work in an integrated manner to support the computer's performance across various aspects of life.

Today, the function of computers is no longer limited to data storage or processing alone. Their development has extended into the realm of digital communication, particularly through the use of the internet. The internet, short for Interconnected Network, is a global network system composed of thousands, even millions, of independent computer networks. As a communication medium, the internet plays a crucial role in accelerating the flow of information across regions without geographical boundaries. Like other conventional media, the internet serves as a channel for delivering messages from sender to receiver. Within computer systems, the human factor—often called brainware—remains a critical element that determines the effectiveness and direction of overall technological development.

A phishing site is a fraudulent webpage created by cybercriminals by imitating an official website's appearance, content, URL address, domain, or other elements to deceive internet users. The primary objective is to make victims believe they are accessing a legitimate site. If the victim is deceived and provides the requested information, the perpetrator can exploit this data to access the real site and carry out harmful actions. The impact of such crimes can be severe, ranging from financial losses to the compromise of personal data.

In the second quarter of 2024, IDADX (Indonesia Anti-Phishing Data Exchange) received 14,093 reports concerning domain abuse submitted by various parties. Of this number, 7,434 cases were identified as misusing short domains belonging to the https://s.id service, which is frequently exploited to disguise malicious or deceptive links. Meanwhile, the remaining 6,659 reports pertained to domain abuse cases involving domains other than https://s.id. These data indicate that short domains such as https://s.id have a high potential for misuse by irresponsible actors. This underscores the need for enhanced monitoring systems and stronger collaboration between domain service providers and regulatory bodies such as IDADX to prevent and address similar incidents of abuse in the future.

According to AKP Nur Wasis, Deputy Head of the Criminal Investigation Unit (Wakasatreskrim) of the Malang City Police Department, continuous coordination is being maintained with the cyber team of Sub-directorate V on Cybercrime, under the Directorate of Special Criminal Investigation of the East Java Regional Police. This is due to the increasing number of cases and the fact that handling them requires a thorough understanding of information technology. Implementing preventive policy measures to create a secure and orderly environment within society has prompted the researcher to conduct a more in-depth analysis of the countermeasures against cyber phishing, which has caused significant losses to victims. This study is entitled "Countermeasures Against Cyber Phishing Crimes Under the Electronic Information and Transactions Law."

RESEARCH METHODOLOGY

The research method employed in this study is the sociological juridical approach, which emphasizes empirical investigation by directly engaging with the research object to obtain a comprehensive understanding of legal implementation and social factors in addressing cyber phishing crimes.

RESEARCH FINDINGS AND DISCUSSION

A. Personnel and Equipment in the Mitigation of Cyber Phishing within the Jurisdiction of the Malang City Police Department.

a. Theoretical Framework

Lawrence Meir Friedman, a prominent legal sociology scholar from Stanford University, asserts that law enforcement consists of three interrelated components: Legal Structure, Legal Substance, and Legal Culture.

First, Legal Substance:

Legal substance is a crucial element in the effectiveness of law. It encompasses legal products such as court decisions and regulations, and the living law—the norms that exist and are practiced within society. The Indonesian legal system, which follows the Civil Law tradition, is based on written rules. It adheres to the principle of legality, as stipulated in Article 1 of the Indonesian Penal Code (KUHP). This principle means that a person can only be punished if their actions are clearly defined and regulated by the prevailing laws and regulations.

Second, Legal Structure:

The legal structure encompasses institutions such as the Police, the Public Prosecutor's Office, the Courts, and Correctional Facilities, all vital in effectively implementing the legal system. As regulated under Law No. 8 of 1981, each institution must operate independently, free from interference by other branches of power. The fiat justitia et pereat mundus principle underscores the importance of upholding justice even under the most challenging circumstances. However, the success of law enforcement is largely dependent on the quality of its legal apparatus. Issues such as low integrity, economic limitations, and non-transparent recruitment processes are among the major obstacles. Without competent and professional law enforcement officers, legal systems cannot function effectively, even if the regulations are ideal.

Third, Legal Culture:

Legal culture reflects the public's attitudes, values, and awareness toward the law. This aspect determines whether the law is obeyed, ignored, or misused. The level of public legal awareness serves as a key indicator of a legal system's effectiveness. In the framework of law, structure functions as the engine, substance as the output, and culture as the guiding force. These three components are deeply interconnected and collectively determine the practical effectiveness of the legal system.

b. Research Findings

The research findings related to the first research question—namely, how personnel and equipment are utilized in the mitigation of cyber phishing crimes within the jurisdiction of the Malang City Police Department—indicate that the presence of competent personnel and adequate equipment is crucial for the effective

DOI: 10.5281/zenodo.16757823

handling of this type of cybercrime. Based on primary data obtained through interviews with members of the Criminal Investigation Unit of the Malang City Police, the personnel involved in cyber phishing mitigation consist of a specialized team with expertise in both information technology and criminal law. These personnel possess a solid understanding of legal aspects and demonstrate technical capabilities in conducting digital investigations, such as IP address tracking, digital footprint analysis, and the lawful collection of electronic evidence.

In addition, the Malang City Police Department has equipped its team with technological tools to investigate cyber phishing offenses. These tools include digital forensic software, network monitoring systems, and hardware capable of accessing and securing electronic data from various sources. However, the interviews revealed that although the current equipment is relatively sufficient, there remains a need to enhance technological capacity to keep pace with the increasingly complex and sophisticated methods used in cybercrime.

From the personnel perspective, regular training and capacity building have become a primary focus to ensure that team members remain up-to-date with the latest techniques in combating cybercrime. The Malang City Police Department routinely conducts training sessions and workshops in collaboration with relevant institutions and experts in the field of information technology. These initiatives aim to enhance personnel's digital analysis and investigative skills, enabling them to identify the modus operandi of cyber phishing perpetrators more accurately and efficiently.

Furthermore, inter-unit coordination within the Malang City Police Department is also critical in addressing this type of crime. Personnel from various divisions, such as Criminal Investigation, Information Technology, and Public Relations, work collaboratively to collect data, conduct investigations, and educate the public on the dangers of cyber phishing and methods of prevention. This synergy strengthens the overall effectiveness of case handling and accelerates the process of law enforcement.

However, the study also identified several challenges related to personnel and equipment. One major issue is the limited number of personnel with expertise in cybercrime, which poses difficulties given the increasing complexity of cases. In addition, budget constraints hinder the procurement of the latest technological tools, which are essential to address the evolving methods employed by cybercriminals effectively. These limitations have the potential to slow down and reduce the accuracy of investigation processes and the enforcement of actions against cyber phishing offenders.

As a solution, the Malang City Police Department seeks to optimize existing resources by prioritizing case handling based on financial loss and social impact. Moreover, efforts to strengthen collaboration with other institutions—such as regional police departments, the National Cyber and Crypto Agency (BSSN), and academic and technological research institutions—are expected to enhance personnel capacity and facilitate upgrading technological equipment. This approach also includes the development of a more accessible reporting and complaint system for the public, aimed at accelerating the detection and response to cyber phishing incidents.

Overall, the research findings indicate that the personnel and equipment at the Malang City Police Department are on the right track in addressing cyber phishing crimes; however, further capacity-building and support through more advanced technology are still required. Enhancing personnel competence through continuous training and the procurement of modern equipment are key strategies in tackling the increasingly complex challenges of cybercrime. Consequently, the Malang City Police Department will be better positioned to provide more effective and responsive legal protection for the public against the threat of cyber phishing within its jurisdiction.

B. Challenges and Solutions Faced by the Malang City Police in Combating Cyber Phishing Crimes

a. Theoretical Framework

The theory of legal effectiveness examines the extent to which law can achieve its primary objective: to regulate societal behavior by prevailing norms and create social order. According to Soerjono Soekanto, a law is considered adequate if it produces a visible positive impact through its implementation—specifically, when the law successfully guides or alters human behavior so that individuals act by the expectations set forth by legal regulations. In other words, legal effectiveness is measured by the law's ability to shape the attitudes and actions of society in line with its intended goals. Law functions not only as a written set of rules, but also as a tool of social engineering, serving as an "agent of change" within society. For law to be effective, it must meet several criteria: it should address the community's needs, be known and understood by the public, and embody concrete principles of justice. Only then can the law be accepted and implemented adequately by society.

According to Soekanto, the effectiveness of law is influenced by five main factors: the substance of the law (the legislation itself), law enforcement officers (those responsible for implementing the law), supporting facilities and infrastructure, the legal culture of society, and other factors related to social conditions. If any of these factors does not function properly, the effectiveness of the law will be diminished.

Moreover, legal effectiveness also depends on the synergy between transparent and fair legal rules, professional law enforcement, and the awareness and active participation of the public. For example, in addressing criminal acts such as cyber phishing, the effectiveness of the law may be hindered by a lack of skilled personnel, inadequate technological infrastructure, and low public awareness of such criminal tactics. Therefore, enhancing human resource capacity, modernizing equipment, and conducting public education are crucial steps to improve the overall effectiveness of the law. Thus, the theory of legal effectiveness emphasizes that law should not merely exist in a formal sense, but must also function effectively in practice, guiding and transforming public behavior by the objectives of the legal system.

b. Research Findings

The study found that the Malang City Police (Polresta Malang Kota) face significant challenges in combating cyber phishing crimes. First, there is a shortage of personnel with specialized expertise in cybercrime. Cyber phishing, which is inherently complex and constantly evolving, requires law enforcement officers who understand legal aspects and possess knowledge of information technology and the latest cybercrime methods. However, the number of personnel with such competencies remains very limited, thereby hindering the investigation and enforcement processes from being carried out effectively. This limitation is evidenced by the increasing number of cyber phishing cases reported in Malang City.

Number of Cyber Phishing Cases

DOI: 10.5281/zenodo.16757823

at the Malang City Police Department in 2021-2024

NUMBER OF CYBER PHISHING CASES AT THE MALANG CITY POICE DEPARTMENT					
YEAR	TOTAL CASES	HANDLED	NOT HANDLED	INVESTIGATION	INVESTIGATION COMPLETED
2021	32	√	X	32	32
2022	41	√	X	41	41
2023	44	√	X	44	44
2024	58	√	X	58	58

As illustrated by the data above, the number of victims reporting cyber phishing crimes has continued to increase yearly. Furthermore, the existing technological infrastructure cannot handle cyber phishing cases effectively. The lack of advanced technology, limited access to software, and the unavailability of digital forensic tools have resulted in slow and less accurate processes of evidence collection and data analysis. This situation negatively affects the success rate in identifying and apprehending cybercriminals.

Third, the low public awareness and digital literacy regarding phishing techniques pose another significant obstacle. Many individuals are still unfamiliar with how phishing works and its risks, making them vulnerable to becoming victims. The lack of education and outreach on digital security contributes to the public's unpreparedness and delayed reporting of incidents to law enforcement authorities.

To address these challenges, the study recommends several strategic solutions. First, enhancing the capacity of personnel through specialized training and education in cybercrime is essential. By improving the competence of law enforcement officers, investigation and enforcement processes can be carried out more effectively and efficiently. Such training should include technical aspects of digital forensics, cyber investigation techniques, and a comprehensive understanding of legal regulations about cybercrime.

Second, the modernization of technological infrastructure is a crucial step. The Malang City Police must adopt the latest technologies that support the collection and analysis of digital evidence, such as advanced forensic software and cyber monitoring systems. Investing in this technological infrastructure will accelerate case handling processes and improve the accuracy of investigations.

Third, increasing public literacy and awareness through intensive outreach and continuous digital education is essential. Educational programs involving various community elements—schools, local communities, and mass media—can help the public understand phishing risks and how to prevent them. With greater awareness, citizens are expected to become more vigilant and proactive in reporting cybercrime incidents to law enforcement authorities.

Fourth, synergy among law enforcement, technology, and society must be strengthened. This integrated approach will improve coordination in preventing and addressing cyber phishing. For instance, collaboration with internet service providers and digital platforms can aid in early detection and rapid blocking of phishing activities.

CONCLUSION

Competent personnel and adequate equipment are crucial in addressing cyber phishing crimes. However, the limited availability of human resources with expertise in cybercrime remains a significant obstacle to the effectiveness of case handling. This limitation highlights that the effectiveness of law enforcement does not solely depend on the existence of legal regulations, but also on the quality of law enforcement officers and public legal awareness, which together form the legal culture that supports the actual implementation of the law. Therefore, combating cyber phishing requires technical, legal, and social synergy to achieve optimal outcomes.

REFERENCES

1. Abdul Manan, Aspek-aspek Pengubah Hukum, Kencana Prenada Media, Jakarta, 2006, Hlm 24-25.
2. Edmon Makarim, Kompilasi Hukum Telematika, (Jakarta Raja Grafindo Persada), 2003, Hal 54.
3. Erwin Ginting, Analisis Ancaman Phising Terhadap Layanan Online Perbankan, Journal of Scientech Reserch. Vol. 8 Issue 1, Juni 2023, Hal 2.
4. Freddy Harris, Pengantar Menanti Hukum Cyberspace, Jurnal Hukum dan Teknologi, Edisi 1 Tahun 1, 2001, Hal 5
5. Indonesia Anti-Phishing Data Exchange, Laporan Aktivitas Abuse Domain.id, http://www.idadx.id/ (Senin, 28 April 2025)
6. Sabian Utsman, Dasar-Dasar Sosiologi Hukum (makna dialog antara Hukum & masyarakat), Pustaka Pelajar, Yogyakarta, 2016, Hlm 180-190.
7. Saputra, A. M. A., Kharisma, L. P. I., Rizal, A. A., Burhan, M. I., & Purnawati, N. W. (2023). TEKNOLOGI INFORMASI: Peranan TI dalam berbagai bidang. PT. Sonpedia Publishing Indonesia.
8. Zainuddin, (2023, 14 Juli), Penanganan Kejahatan Phising di Malang, Polisi Kerahkan Tim IT, https://suryamalang.tribunnews.com/2023/07/14/penanganan-kejahatan-phising-di-malang-polisi-kerahkan-tim-it (Diakses pada 5 Mei 2025)

DOI: 10.5281/zenodo.16757823