International Journal of Safety and Security Engineering
Vol. 14, No. 6, December, 2024, pp. 1699-1706
Journal homepage: http://iieta.org/journals/ijsse

Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities

Wardah Yuspin[1*], Alda Oktalivia Putri[1], Ata Fauzie[2], Jompon Pitaksantayothin[3]

[1] Faculty of Law, Universitas Muhammadiyah Surakarta, Surakarta 57162, Indonesia
[2] Faculty of Islamic Studies, Universitas Muhammadiyah Surakarta, Surakarta 57162, Indonesia
[3] Institute for EU Studies and Center for Southeast Asian Studies, Hankuk University of Foreign Studies, Seoul 02450, Republic of South Korea

Corresponding Author Email: wy204@ums.ac.id

https://doi.org/10.18280/ijsse.140605

Received: 17 May 2024
Revised: 14 July 2024
Accepted: 1 August 2024
Available online: 31 December 2024

Keywords:
digital bank, fraudulent, phishing, prevention, security

ABSTRACT

This research aims to explore the industry's transition towards digitalization, with a particular focus on the banking security's shift towards digital banks. However, this growth is accompanied by threats stemming from inadequate personal data protection, which could negatively impact the development of digital banking services. This includes the practice of phishing, a method used to steal user information with the intent of obtaining a user ID or password. This research, therefore, adopts a qualitative legal approach. The data sources for this research include both primary and secondary data. The findings reveal that, according to Lawrence M. Friedman's theory, the legal system consists of three main components, namely legal structure, legal substance and legal culture. These three components interact and influence each other in shaping the effectiveness of a legal system. According to the theory the legal regulations regarding phishing in Indonesia are not yet optimally effective. This can be observed from the existing legislation and law enforcement factors, which play a crucial role in the functioning of the law but have not been successful in reducing phishing cases in Indonesia.

1. INTRODUCTION

Industries are progressively transitioning towards digital platforms, promoting the adoption of diverse activities to align with these advancements [1]. The rapid development of technology and the increasing human needs are both pushing the boundaries of space and time [2]. Technological innovation, besides providing comfort in life, also contributes to transformation in the financial sector, which is currently undergoing significant changes, particularly in the banking sector.

As a country still in the development stage, Indonesia can be recognized through numerous development programs spread across various sectors of national and state life, specifically in the context of Internet media. This is reflected in the increasing use of communication tools and technology, such as computers, laptops, mobile phones, and the internet, which are progressively becoming widespread in society [3]. Technological advances have made a positive contribution by facilitating more effective communication and simplifying complex tasks. These advances have led to the creation of digital banking, which has transformed the way people interact with financial institutions and brought more choice and convenience to managing their personal finances. Utilising digital technology is a means to meet customer needs in the face of rapid developments in the digital economy. Eleven digital banks are currently operating in Indonesia, including Bank Jago, Blu, Jenius, Livin, Neo Bank, Allo Bank, Linee Bank, Motion Bank, Bank Raya, and D-Save [4].

Nevertheless, advancement, especially in the field of internet media as a means of widespread information dissemination, has serious implications in the form of misuse. Certain parties can utilise internet media to gain profits by stealing personal data, including user IDs or passwords, through phishing practices. Phishing is an act of fraud carried out by irresponsible parties with the intention of stealing personal data. This involves obtaining data such as user ID or password (internet access key), PIN (user and system secret password), account number, and credit card numbers, unlawfully via fraudulent emails claiming to be legitimate business entities to individuals, companies, or organisations.

Fraudulent activities are documented in police data on the PUSIKNAS (National Criminal Information Center) website. In 2022, there were 33,167 reported fraud cases, and in 2023, this number rose to 35,425, totalling 68,592 cases. According to 2022 reports, the Cyber Crime Directorate of the Indonesian Police Criminal Investigation Agency (Bareskrim Polri) recorded 5,579 incidents.

In the banking industry, one of the most important things to keep in mind is phishing. The goal of phishing attempts is to obtain as much information as possible from victims. Through the appearance of a reliable source, phishing assaults attempt

to deceive victims. This is done in an attempt to coerce the victim into disclosing personal information and other sensitive data. Phishing attempts aim to gain usernames, passwords, and card information in the banking industry. Phishing involves posing as a reliable website and making official-sounding statements. Phishing assaults come in various forms that trick their victims: (1) phishing emails, (2) phishing calls, (3) phishing website impersonations, and (4) phishing social media posts [5].

Phishing attacks saw an increase of approximately 41.52% compared to the previous quarter, amounting to 3,942 attacks. Among various banking and financial institution products, e-wallets and bank accounts are considered most susceptible to potential data breaches. Presently, there is a surge in phishing cases in banking, with methods that deceive customers by appearing as official messages from the bank [6].

For instance, several customers of Jenius National Pension Savings Bank (BTPN) experienced suspicions of personal data leakage. This issue arose when customers received phone calls, allegedly from Jenius, informing them about replacing their debit cards. Initially, customers did not suspect anything amiss as the caller's manner of speaking resembled that of Jenius' usual customer service. Unwittingly, the customer followed the link provided by the caller. Shortly thereafter, the customer's Jenius application abruptly logged out, and the customer was unable to log back in. Upon seeking information at the BTPN office, customers discovered that a significant amount of their money had been transferred to another account. This incident raised concerns that BTPN Jenius customers' personal data had been leaked and used unlawfully, resulting in financial losses to customers [7].

Furthermore, Mochamad Riza Achrullah, Head of Information Technology Security at Allo Bank, disclosed that cybercrime also poses threats to digital banks such as Allo Bank. A customer narrowly avoided becoming a victim of fraud when they received a call from the United States concerning changes to transfer rates. Despite suspicions of potential fraud, the customer contacted Allo Bank, thereby evading attempts to obtain personal data by the perpetrator. In response, Allo Bank's cybersecurity team issued a warning to customers to maintain the security of personal data and implemented a real-time cybersecurity and monitoring system.

Based on data collated by the Indonesia Anti-Phishing Data Exchange (IDADX), overseen by the Indonesian Internet Domain manager, there were 88,822 phishing reports over the past five years, starting from 2018. The number of unique phishing attacks reported in the Q1-Q4 2022 period amounted to 22,853. In contrast, the number of phishing attacks reported in the Q1-Q2 2023 period escalated to 47,005. The sector most frequently targeted by phishing from the first quarter to the second quarter was social media, accounting for 53.95% of all attacks. This year, phishing reports have surged every quarter compared to previous years, reflecting an increase of up to four times.

A review of prior research was undertaken with the objective of obtaining comparative and reference material. This was done to circumvent any impression of overlap with current research. Therefore, in this literature review, the researchers documented findings from previous studies.

Radiansyah et al. [8] in their research titled "Analysis of Phishing Threats in Online Banking Services," utilised the Systematic Literature Review (SLR) method. SLR, also known as Systematic Review, is a type of literature review that researchers typically employ to address problems in research. The research findings revealed the factors contributing to the emergence of phishing and the strategies for preventing phishing threats. Based on the results of previous literature studies, the factors leading to the emergence of phishing threats include the use of online banking services by users, lack of knowledge, and social and psychological privacy [8].

In her research, Widayanti [9] examined "Criminal Acts of Theft of Customer Data in the Banking Sector as Cybercrime." The research employed a normative method with a deductive logical reasoning approach. The research findings indicated several modes of operation in stealing customers' personal data by cybercrime, which often occurs in the banking sector, and one of them is phishing. There are two steps to prevent criminal acts of theft of personal data in the banking sector: the first is a penal policy, and the second is non-penal policy prevention carried out without invoking criminal provisions, such as enhancing the security system in the banking world.

Additionally, Dm et al.'s [10] research entitled "Phishing Crimes in the World of Cybercrime and the Legal System in Indonesia" employed normative research methods with a descriptive approach to explore various aspects of laws and regulations relating to cybercrime crimes. Sources of phishing threats included email, websites, and Malware. Then, preventions of the phishing attacks mentioned were detected with detection tools using anti-tab nabbing web browser add-ons, pre-filter mechanisms, and self-efficacy.

The article aims to investigate the efficacy of Indonesia's phishing prevention regulation. This measure is implemented to prevent fraud inside the sector, particularly in digital banking. Based on the background the problem formulation is How effective are the regulations on phishing can prevent fraudulent particularly in digital banking?

2. METHOD

This research uses a qualitative legal approach by studying legislation, theories, and concepts related to the problem under study [11]. The data collection process is carried out through library research, with primary legal materials consisting of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 regarding Electronic Information and Transactions (ITE Law), and Article 378 of the Criminal Code. Secondary legal materials are sourced from the opinions of legal experts and journals relevant to the topic or previous research related to the problem under study. Secondary legal materials are sourced from the views of legal experts and scientific articles pertinent to the topic or previous research related to the problem under study.

3. RESULTS AND DISCUSSION

3.1 Legal regulations on phishing attacks threatening personal data theft in digital banks

In accordance with Financial Services Authority Regulation (POJK) No.12/POJK.03/2021, digital banks are defined as banking institutions officially registered in Indonesia that predominantly conduct their banking activities through electronic platforms, without relying on physical branches beyond the head office or maintaining a very limited number of physical branches. Financial Services Authority Regulation Number 12/POJK.03/2021 and Financial Services Authority

Regulation Number 12/POJK.03/2018 pertain to digital banks in Indonesia, addressing commercial banks and the provision of digital banking services by these entities.

The advent of digital banking heralds a reduction in operational costs, constituting a significant long-term investment in the banking landscape [12]. Banking institutions stand to expand their market share by curbing expenditures required for establishing additional physical branches and cash offices. The transition to a digital bank, where technology permeates the financial infrastructure, yields substantial time-saving benefits [13]. Procedures become streamlined and more user-friendly, eliminating the necessity for in-person branch visits. Customers can open accounts in under ten minutes through the application interface, facilitating swift and straightforward navigation. Accessibility is enhanced, enabling round-the-clock banking services from diverse locations [14]. Various incentives, such as cashback rewards, points redeemable for discount vouchers, and attractive interest rate offers, further enhance the appeal of digital banking [15].

Nevertheless, according to OJK notes, several obstacles may be faced in the future digital banking transformation process, i.e., challenges in the use of artificial intelligence technology in the banking sector, including several risks [16]. Artificial intelligence has been applied in various aspects of banking, like automation of tasks, such as fraud detection [17], identification of money laundering transactions, or reversal decisions in credit card applications, which can carry risks in the context of artificial intelligence, including algorithmic bias [18, 19]. The protection of personal data and the risk of losing customer information are vital aspects [20]. According to OJK, protecting customers' personal data will have a significant impact on the development of digital banking services in the future [21, 22].

Data protection is a pivotal element in fostering trust in online transactions and plays an integral role in the digital transaction environment. Threats stemming from weak personal data protection can adversely impact the growth of digital banking services [23]. One of the primary reasons is the lack of an adequate legal framework governing the protection of personal data, resulting in local companies not being fully compliant with data protection standards, the use of deepfakes, and the ability to make independent decisions [24]. Moreover, the low level of financial literacy also poses a challenge. According to the Financial Services Authority (OJK), a deficiency in understanding digital financial literacy among bank consumers can trigger cybercrime. As per the data recorded by the Cyber Crime Directorate, Bareskrim Polri, from January to September 2020, there were 2,259 public reports regarding digital crime. The report includes hacking of electronic systems, online fraud, data or identity theft, and data manipulation. Online fraud is the most frequent complaint, indicating a lack of public understanding of the risks involved in digital transactions. Cyber threats (cybercrime) also pose a significant risk. Data from the BSSN National Cyber Security Operations Center reveals a substantial increase in the number of cyberattacks, with 495 million cyberattacks in 2020, a five-fold increase compared to the previous year (228 million cyberattacks). Therefore, digital banks need to prioritize strong cybersecurity [25].

In this context, Act Number 27 of 2022 on Personal Data Protection (PDP Act) serves as a legislative instrument designed to protect the personal data of Indonesian citizens from misuse, including phishing practices [26]. The provisions for personal data protection are enshrined in Article 28G of the 1945 Constitution of the Republic of Indonesia, which emphasizes the right to protection of personal data, family, honor, dignity, and property under its jurisdiction. Furthermore, the definition of personal data is outlined in Act Number 27 of 2022 on Personal Data Protection, Article 1, Section 1, clarifying that personal data refers to information about individuals who can be identified, either independently or in conjunction with other data, through electronic and non-electronic systems. Privacy safeguarding forms an integral aspect of personal data protection, as explicitly mandated by the Constitution of the Republic of Indonesia, embodying respect for human rights principles and the equitable treatment of individuals, thereby necessitating legislative intervention [27].

This regulation is rooted in the principles of human rights and the ethos of equality and respect for individual rights, with the overarching aim of ensuring the privacy and security of individuals' personal data, including those who are customers or borrowers [28]. Phishing attacks emerge as one of the catalysts for crimes involving the misappropriation of personal information. These attacks can be perpetrated relatively effortlessly and at minimal expense. Perpetrators have the capacity to disseminate thousands or even millions of emails or text messages rapidly in their attempts to defraud individuals [29]. Phishing constitutes a criminal offence that employs both social engineering techniques and tactics aimed at illicitly acquiring an individual's personal identity data and financial account credentials [30].

Phishing, dating back to as early as 1996, is far from a recent phenomenon, casting a long shadow over digital realms [31]. Consequently, this study undertakes an examination of the legal frameworks encircling phishing attacks, which pose a grave threat to the integrity of personal data. Particularly within the domain of banking, a pressing concern manifests in the illicit acquisition of customer accounts within digital banking platforms [32]. A prime example of this nefarious practice is the fabrication of spurious bank accounts in Indonesia, coupled with the dissemination of deceptive websites masquerading as legitimate entities, ostensibly offering online credit or administrative fee discounts to unsuspecting customers. Undoubtedly, phishing epitomizes a quintessential cybercrime [33].

The legal statutes governing cybercrime, specifically phishing, in Indonesia demand meticulous scrutiny, with penalties delineated under Article 378 of the Criminal Code. This provision is tailored to address acts of fraud, with phishing intrinsically aligned with fraudulent activities. Fraud, as outlined in Article 378, encompasses actions wherein individuals, harbouring the intent to unlawfully benefit themselves or others, resort to false identities or pretences, thereby coaxing others into surrendering property, incurring debts, or absolving liabilities [34]. The application of Article 378 in prosecuting cybercrimes necessitates a nuanced interpretation, acknowledging the nuances that differentiate cyber-enabled offences from conventional criminality. While parallels may be drawn between the modus operandi of phishing and traditional fraud, significant disparities manifest in the nature of the offences, the determination of crime locales (locus delicti), and the temporal aspect of criminal acts (tempos delicti) [35].

The intricate process of phishing involves a sequence of orchestrated steps by the perpetrator, commencing with the dissemination of counterfeit messages via email, short

message service (SMS), or fraudulent websites targeted at specific individuals. These messages commonly solicit sensitive personal information, including user IDs, PINs, or credit card numbers, from unsuspecting recipients. Phishing criminals frequently employ tactics to induce a sense of urgency, imposing tight deadlines for the provision of requested data, often accompanied by veiled threats of adverse consequences should compliance not be immediate. In such scenarios, individuals who act impulsively, without due deliberation, become more susceptible to divulging personal information to fraudsters [36].

The data acquired from victims can then be nefariously exploited by perpetrators, with personal information potentially leveraged to deplete customer balances or engage in other fraudulent activities [25]. Although phishing attempts are typically clandestine and challenging to discern, several telltale signs can serve as red flags. Notably, phishing messages often exhibit rudimentary or foreign language usage, imparting a tone that may appear brusque or linguistically discordant. This linguistic irregularity frequently serves as an initial indicator hinting at potentially fraudulent activity. Moreover, disparities in the visual presentation of banking websites constitute another notable indicator. While counterfeit banking sites may superficially resemble authentic counterparts in terms of web icons or menu displays, meticulous scrutiny may reveal subtle inconsistencies indicative of their illegitimacy [37].

Legal regulations concerning phishing cases encompass a range of motives, unequivocally posing significant harm to consumers [38]. The regulatory framework addressing phishing is comprehensively delineated in Act Number 19 of 2016, amending Act Number 11 of 2008. Article 28, Section (1) of this legislation pertains to the intentional dissemination of false and misleading information leading to consumer losses in electronic transactions. Similarly, Article 30, Section (1) addresses the unlawful and intentional access of another person's computer or electronic system. Furthermore, Article 31, Section (1) concerns the interception of electronic information and/or documents without right or legal authority. Finally, Article 35 encompasses the intentional manipulation, creation, alteration, deletion, or destruction of electronic information and/or documents with the intent to misrepresent them as authentic data.

Additionally, Article 36 of the ITE Act stipulates that individuals who intentionally and unlawfully commit acts outlined in Articles 27 to 34 resulting in harm to others shall be held accountable. Furthermore, Article 45A, Section (1) prescribes penalties for those who distribute electronic documents containing indecent content, with a maximum punishment of six years imprisonment and/or a fine of up to IDR 1,000,000,000.

Act Number 19 of 2016 introduces clarifications to Article 5, Sections (1) and (2), which previously were deemed self-explanatory. The added elucidation in Section (1) recognizes electronic information and/or documents as legally binding evidence, ensuring certainty in electronic transactions and systems. Moreover, Section (2) specifies that interception, tapping, or recording of electronic information and/or documents, particularly in the context of wiretapping, must occur within the bounds of law enforcement at the behest of authorized entities such as the police or prosecutor's office.

Furthermore, the Information and Electronic Transactions Act (UU ITE) primarily focuses on resolving cases through the imposition of criminal sanctions, including imprisonment and fines, as delineated in Article 45A, Section (1) of the ITE Act. The punitive measures aim to enforce the law and deter future criminal activity, with imprisonment and fines serving as common sanctions across both the ITE Act and the Criminal Code. However, the efficacy of such punitive measures in ensuring material compensation for victims, especially in the context of cybercrimes where victims' financial security is compromised, is debatable [39].

Moreover, every citizen's right to fair legal protection necessitates a nuanced approach, particularly in the realm of cybercrime [40]. Challenges faced by investigators due to the rapid evolution of information technology and electronic transactions, coupled with perpetrators' adeptness at concealing evidence, underscore the need for adaptations in legal provisions. Act Number 19 of 2016 addresses these challenges by amending several provisions related to the investigation of criminal acts in the field of information technology and electronic transactions, as elucidated in the general explanation in the concluding section [41].

Moreover, offering restitution to victims of cybercrime, such as phishing, is a suitable course of action. This is outlined in Article 1, Point 11, which defines restitution as compensation provided by the perpetrator or a third party to the victim or their family. Similarly, Article 1, Point 8 of Act Number 31 of 2014, amending Act Number 13 of 2006 on the Protection of Witnesses and Victims, stipulates protection as the fulfillment of rights and provision of assistance to ensure the security of witnesses and/or victims in accordance with legislative provisions. However, witness and victim protection regulations remain discretionary, subject to the Witness Protection Agency's (LPSK) decision to guarantee the realization of their rights. Furthermore, the legislation lacks detailed delineation regarding the types of crimes eligible for restitution, thereby engendering uncertainty for victims. Additionally, the Criminal Code does not provide specific provisions for criminal compensation. Article 14C of the Criminal Code, concerning conditional sentences, primarily serves as an alternative to the principal punishment rather than a compensation mechanism. Notably, the imposition of special conditions, such as compensation, in cases involving conditional sentences falls within the purview of the judge, contingent upon a maximum prison sentence of one year or imprisonment. However, the application of such conditions remains discretionary [42].

3.2 The efficacy of the regulations governing phishing attacks

The effectiveness of Act Number 19 of 2016 on Electronic Information and Transactions in achieving its stated objectives, particularly in realizing justice, public order, and legal certainty, warrants examination through specific criteria within the context of electronic information and transactions. These criteria can be elucidated by Lawrence M. Friedman’s Legal System Theory, which posits that the success of law enforcement hinges upon three key elements: the structure of the law, the substance of the law, and the legal culture. The structural aspect of the law pertains to the framework of institutions within the legal system, each fulfilling distinct functions to facilitate its operation [43].

According to Friedman, these institutions collectively form the legal infrastructure, delineating overarching structure and boundaries. Key components of this structural framework include law enforcement entities such as the police,

prosecutor's office, courts, and community institutions. Conversely, the substance of the law encompasses the norms, behavioural patterns, and written legal rules governing society. Referring to the theories of H.L.A. Hart, Friedman delineates the substance of law as comprising rules and regulations that govern institutional behaviour and conduct. Furthermore, the concept of legal culture encapsulates human attitudes towards the law, elucidating how the law is perceived, utilised, or circumvented within society. These attitudes significantly influence the application and adherence to legal principles and regulations.

The effectiveness of the legal system in addressing crime within society is heavily contingent upon the three aforementioned aspects. By mitigating potential weaknesses in these dimensions, criminal law enforcement can optimise outcomes in resolving cases of crime within society. This principle holds true for criminal law enforcement concerning cybercrimes, where these aspects wield significant influence. Law enforcement plays a pivotal role in the functionality of the legal system, and combating cybercrime hinges upon the existence of statutory regulations, particularly those pertaining to laws concerning information technology in the context of internet-related offences. Moreover, in handling cybercrime cases, law enforcement officials must accord due attention to the digital evidence utilised by perpetrators in executing their illicit activities. Digital evidence assumes paramount importance in the evidentiary process during court proceedings, thereby necessitating its meticulous handling by law enforcement personnel. The judicial panel relies upon digital evidence in cybercrime cases to adjudicate effectively, underlining its indispensable role in the judicial process [44].

However, enforcement of regulations relating to cybercrime, particularly phishing methods, still needs to be improved, as evidenced by the increasing number of phishing cases reported annually in Figure 1. Phishing crimes have increased, infiltrating various banking websites, including digital banks. Several obstacles contribute to this trend, including challenges in law enforcement stemming from a lack of understanding of internet technology, uneven distribution of technology or infrastructure, and socio-economic factors related to societal and cultural dynamics. This needs to be fully supported, especially in regulations to provide legal protection for victims and strict sanctions for perpetrators. Therefore, there is a need for amendments to the regulation.

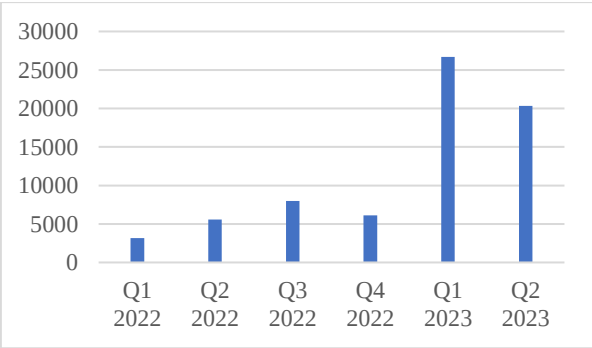

Figure 1. Phishing report in Indonesia 2022-2023

These factors collectively hinder the optimal implementation of laws pertaining to information and electronic transactions, fostering a perception of phishing as a commonplace occurrence and perpetuating the belief that fraud and data theft offer easy pathways to profit [45].

The legislative framework governing law enforcement for phishing crimes lacks uniformity, primarily due to phishing encompassing various criminal modalities, including cybercrime, fraud, and personal data theft. Act Number 19 of 2016 on Information and Electronic Transactions serves as the primary legislative instrument aimed at curtailing the incidence of phishing attacks. However, weaknesses persist within this regulatory framework. If phishing crimes involve more than one jurisdiction of different countries, the obstacles faced can complicate the law enforcement process, making it very complicated, for example, in the collection of digital evidence. It is very complicated, for example, in the collection of digital evidence. Phishing crimes occur due to legal uncertainty in the application of the laws used, especially if the crime involves the jurisdiction of another country. This requires solid international cooperation through special laws to tackle phishing crimes. Particularly concerning sanctions, ambiguity clouds its enforcement. Statutory regulations delineate penalties imposed by judges for phishing crimes, such as imprisonment for specified durations, as outlined in Act Number 27 of 2022 on Personal Data Protection (PDP Act). While existing phishing regulations are reasonably detailed, they still harbour loopholes that undermine their effectiveness.

Furthermore, legal culture encompasses the prevailing social attitudes and influences that shape how the law is applied, circumvented, or misused within a society. The connection between legal culture and public legal awareness is of immense significance, as heightened legal awareness within society fosters the cultivation of a more positive legal culture. A positive legal culture has the potential to reshape individuals' perceptions of existing laws. However, one pivotal factor influencing the efficacy of customer legal protection against phishing crimes in the banking sector is privacy culture. Evidence of the persistently weak legal culture can be observed in various cases where individuals readily divulge sensitive information when contacted under the pretext of banking verification requests. This phenomenon underscores a prevalent lack of digital literacy among the majority of the Indonesian populace, with many individuals lacking proficiency in technology usage and understanding its associated risks and potentials. Cybersecurity challenges, coupled with a pervasive lack of awareness regarding cyber threats and attacks, further compound the erosion of technology culture in Indonesia. Consequently, a lack of awareness regarding cybercrime permeates society, reflecting a pressing need for enhanced digital literacy initiatives [46].

In this context, digital banks provide a comprehensive array of services and facilities exclusively via online platforms. The advent of digital banks enables customers to execute financial transactions and manage banking affairs swiftly, at their convenience, and from any location. With the rise of digital banking, the necessity for customers to interact with tellers or depend on the proximity of physical branch offices has been eliminated. The defining criteria for digital banks encompass the assurance of a seamless and unimpeded banking process that prioritises customer convenience. As a result, customers of digital banks can avail banking services without the requirement to physically visit a branch, thereby facilitating effortless interaction and engagement with others in close proximity using merely a smartphone and an internet connection. Consequently, digital banks have emerged as an attractive alternative for various segments of the population. This transformation is indicative of the paradigm shift in the banking sector, driven by the relentless pursuit of customer

convenience and technological advancement [47].

When assessing the efficacy of digital banks in direct customer relationships, it becomes apparent that the absence of physical interaction potentially heightens the risk of phishing attacks compared to conventional banks. This vulnerability arises from a lack of awareness among individuals, as customers may not exercise sufficient vigilance against phishing threats and can easily fall prey to fraudulent messages purportedly originating from digital banking institutions. While banks diligently strive to mitigate the risk of phishing attacks, digital banks must continually enhance customer education regarding this threat, fortify their security measures, and actively monitor suspicious activities. Customers, too, bear responsibility by maintaining vigilance, refraining from clicking on suspicious links, and avoiding careless disclosure of personal information [48].

In Indonesia, the government's role in combatting phishing is primarily manifested through the Personal Data Protection (PDP) Act. This legislation underscores the government's commitment to safeguarding individuals' personal data against phishing crimes [49]. However, despite the enactment of this law, many individuals and organizations remain unaware of its provisions and lack knowledge regarding precautionary measures to protect personal data [50]. Given the relative novelty of this legislation, the government must conduct extensive outreach efforts across the region to ensure that government institutions, legal entities, and the general public comprehend their rights and responsibilities and understand how to report unauthorized data collection by other parties. In the contemporary digital landscape, personal data holds significant value and is frequently exploited by malicious entities. Therefore, the PDP Act represents a crucial stride towards safeguarding privacy and individual rights concerning the collection, usage, and dissemination of personal data [46].

When evaluating the effectiveness of the aforementioned phishing reports, we can cautiously categorize them as moderately effective. The Personal Data Protection (PDP) Act, which aims to enhance the safeguarding of customers' personal data, plays a pivotal role in this context. However, when scrutinizing the efficacy of this legislation through the lens of Lawrence M. Friedman's theory, certain deficiencies become apparent, particularly concerning the law's structural framework. The persistent rise in phishing cases each year, especially as digital financial platforms attract a growing user base, underscores the need for robust legal mechanisms. Law enforcement assumes a critical role in administering the legal system, particularly in combatting cybercrime—a domain closely intertwined with statutory regulations, especially those related to information technology and internet-based offenses. However, several obstacles hinder effective law enforcement. These include limited understanding of internet technology, disparities in technology distribution, and socio-economic factors.

Furthermore, non-compliance with Act Number 19 of 2016 on Information and Electronic Transactions highlights suboptimal implementation of regulations pertaining to phishing crimes [51]. The substance of these laws exhibits ambiguity and weaknesses. Enforcers often lack comprehensive comprehension, reflected in inadequate digital literacy levels and a general lack of technological proficiency among the Indonesian populace. Insufficient awareness of cybersecurity issues and cyberattacks further jeopardizes Indonesia's technological landscape. Addressing these deficiencies is imperative for bolstering the effectiveness of legal frameworks governing cybercrime and enhancing nationwide cybersecurity measures [52]. As the digital landscape evolves, proactive efforts to bridge knowledge gaps and strengthen enforcement mechanisms are essential to safeguard privacy and combat cyber threats effectively [53].

4. CONCLUSIONS

The digitalization trend within the banking industry has yielded both positive and negative consequences, particularly concerning personal data security. While digitalization has ushered in convenience and efficiency in banking services, enabling easier access for customers, it has also led to a surge in phishing attacks and personal data fraud, posing significant security risks and resulting in substantial instances of fraud. Legal regulations in Indonesia, such as Act Number 19 of 2016 on Information and Electronic Transactions and Act Number 27 of 2022 on Personal Data Protection, aim to address various aspects of cybercrime, including phishing.

Examining Lawrence M. Friedman's theory, let us first consider the structure of law related to law enforcement concerning phishing crimes. It reveals a lack of public compliance with existing regulations. Strengthening the structure of law enforcement is imperative. Simultaneously, the substance of the law, exemplified by the Personal Data Protection (PDP) Act, assumes a crucial role in safeguarding personal data. However, weaknesses persist in the application of regulations, particularly in the realm of sanctions, which remain inadequately stringent. Furthermore, cultural factors, such as low digital literacy and insufficient awareness of cybersecurity, pose additional hurdles to effective law enforcement against phishing.

Among these three elements, law enforcement, regulatory frameworks, and privacy culture, it is evident that the current state is marked by ineffectiveness. Further rules that could serve as legal protection for victims of phishing schemes must be improved. The PDP Law exists to contribute sufficiently to the formation of a cyber security legal framework. However, comprehensive outreach initiatives are necessary to ensure that all stakeholders comprehend their rights and responsibilities. Furthermore, while digital banking enhances transactional convenience, the absence of direct customer interaction heightens the risk of phishing attacks. Educating customers, improving security measures, and vigilantly monitoring suspicious activities are pivotal in mitigating the risk of phishing attacks in digital banking. In conclusion, concerted efforts are warranted to enhance legal awareness, safeguard personal data, and reduce cybercrime risks, particularly within the digital banking sphere. Moreover, continual updates and enhancements in legal frameworks and law enforcement practices are indispensable in addressing emerging challenges as technology evolves and cybercriminal methodologies become increasingly sophisticated.

REFERENCES

[1] Fajri, M.Z.N., Muhammad, A.A., Umam, K., Putri, L.P., Ramadhan, M.A. (2022). The effect COVID-19 and sectoral financing on Islamic bank profitability in Indonesia. Journal of Islamic Economic Laws, 5(1): 38-60. https://doi.org/10.23917/jisel.v5i1.17181

[2] Agustin, F., Muhtadi, R., Sahal, S. (2023). The

importance of implementing environment, social and government (ESG) and Maqasid sharia-based Islamic finance in Islamic bank. JISEL Journal of Islamic Economic Laws, 6(2). https://doi.org/10.23917/jisel.v6i2.21214

[3] Yuspin, W., Fauzie, A. (2023). Good corporate governance in sharia fintech: Challenges and opportunities in the digital era. Quality - Access to Success, 24(196): 221-229. https://doi.org/10.47750/QAS/24.196.28

[4] Sicillia, M., Yazid, A. (2020). Analisis dampak digital banking dan kualitas pelayanan terhadap kepuasan nasabah pada sebuah bank swasta. Jurnal Pemasaran Kompetitif, 3(2): 79. https://doi.org/10.32493/jpkpk.v3i2.4520

[5] Izzati, F., Rikzan, F., Zolkipli, M.F. (2023). A study of phishing attack towards online banking. Borneo International Journal, 6(1): 65-72.

[6] Ekayani, L., Djanggih, H. (2023). Perlindungan hukum nasabah terhadap kejahatan pencurian data pribadi (phising) di lingkungan perbankan. Journal of Philosophy (JLP), 4(1): 22-40. https://doi.org/10.52103/jlp.v4i1.1485

[7] Yosefine, R.S. Agustina, Agus, D. (2023). Perlindungan hukum terhadap nasabah btpn jenius akibat tindakan phishing (studi kasus bank tabungan pensiunan nasional jenius). Yustisia Tirtayasa, 3(19): 57-72. http://doi.org/10.51825/yta.v2i1

[8] Radiansyah, I., Candiawan, Priyadi, Y. (2016). Analisis ancaman phising dalam layanan online banking. Ekonomika-Bisnis, 7(1): 1-14. https://doi.org/10.22219/jibe.v7i1.3083

[9] Widayanti, P.W. (2022). Tindak pidana pencurian data nasabah dalam bidang perbankan sebagai cyber crime. Legacy: Jurnal Hukum Dan Perundang-Undangan, 2(2): 1-21. https://doi.org/10.21274/legacy.2022.2.2.1-21

[10] Dm, M.Y., Addermi, Lim, J. (2022). Kejahatan phising dalam dunia cyber crime dan sistem hukum di Indonesia. Jurnal Pendidikan dan Konseling, 4(5): 8018-8023. https://doi.org/10.31004/jpdk.v4i5.7977

[11] Zulfikar, Z., Purbasari, H., Puspawati, D. (2021). Exploration study of sharia corporate exploration study of sharia corporate governance disclosure on bank annual governance disclosure on bank annual report of sharia business unit report of sharia business unit. Riset Akuntansi dan Keuangan Indonesia, 6(1): 50-61.

[12] Aziz, N., Rodiah, R., Susanto, H. (2021). Encrypting of digital banking transaction records: An blockchain cryptography security approach. International Journal Computer Applied, 174(24): 21-26. https://doi.org/10.5120/ijca2021921147

[13] Sekhar, C., Kumar, M. (2023). An overview of cyber security in digital banking sector. East Asian Journal of Multidisciplinary Research, 2(1): 43-52. https://doi.org/10.55927/eajmr.v2i1.1671

[14] Vishnuvardhan, B., Manjula, B., Lakshman Naik, R. (2020). A study of digital banking: Security issues and challenges. In Proceedings of the Third International Conference on Computational Intelligence and Informatics, pp. 163-185. https://doi.org/10.1007/978-981-15-1480-7_14

[15] Susanto, S.A., Manek, M.V., Setiawan, R.A., Mustikasari, F. (2023). Customer experience in digital banking: The influence of convenience, security, and usefulness on customer satisfaction and customer loyalty in Indonesia. Journal of Research and Community Service, 4(8): 1671-1685. https://doi.org/10.59188/devotion.v4i8.544

[16] Jakšič, M., Marinč, M. (2019). Relationship banking and information technology: The role of artificial intelligence and FinTech. Risk Management, 21(1): 1-18. https://doi.org/10.1057/s41283-018-0039-y

[17] Ashta, A., Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. Strategic Change, 30(3): 211-222. https://doi.org/10.1002/jsc.2404

[18] Wodo, W., Stygar, D., Błaśkiewicz, P. (2021). Security issues of electronic and mobile banking. In Proceedings of the 18th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, pp. 631-638. https://doi.org/10.5220/0010466606310638

[19] Yuspin, W., Wardiono, K., Budiono, A., Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. Legality: Jurnal Ilmiah Hukum, 30(2): 267-282. https://doi.org/10.22219/ljih.v30i2.23051

[20] Johri, A., Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. Human Behavior and Emerging Technologies, 2023(1): 2103442. https://doi.org/10.1155/2023/2103442

[21] Fang, L., Quintos, D.G. (2023). Security measures applied on digital banking towards service improvement proposal. Journal of Business and Management Studies, 5(5): 47-77. https://doi.org/10.32996/jbms.2023.5.5.5

[22] Tarigan, H.A.A.B., Paulus, D.H. (2019). Perlindungan hukum terhadap nasabah atas penyelenggaraan layanan perbankan digital. Jurnal Pembangunan Hukum Indonesia, 1(3): 294-307. https://doi.org/10.14710/jphi.v1i3.294-307

[23] Musyaffi, A.M., Johari, R.J., Sobirov, B., Oli, M.C., Rahmi, Afriadi, B. (2024). Examining initial trust in adoption of digital banking platform: A personal innovativeness and security perspective. Journal of System and Management Sciences, 14(1): 67-86. https://doi.org/10.33168/JSMS.2024.0105

[24] Patel, Y., Tanwar, S., Gupta, R., Bhattacharya, P., Davidson, I.E., Nyameko, R., Aluvala, S., Vimal, V. (2023). Deepfake generation and detection: Case study and challenges. IEEE Access, 11: 143296-143323. https://doi.org/10.1109/ACCESS.2023.3342107

[25] Udayakumar, R., Joshi, A., Boomiga, S.S., Sugumar, R. (2023). Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. Journal of Internet Services and Information Security, 13(4): 138-157. https://doi.org/10.58346/JISIS.2023.I4.010

[26] Sudarwanto, A.S., Kharisma, D.B.B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4): 1443-1457. https://doi.org/10.1108/JFC-09-2021-0193

[27] Prastyanti, R.A., Rahayu, I., Yafi, E., Wardiono, K., Budiono, A. (2022). Law and personal data: Offering strategies for consumer protection in new normal

situation in Indonesia. Jurnal Jurisprudence, 11(1): 82-99. https://doi.org/10.23917/jurisprudence.v11i1.14756
[28] Zinovieva, V., Shchelokov, M., Litvinovsky, E. (2023). Legal issues of protection of personal data: Cases of transport data leaks. Transportation Research Procedia, 68: 461-467. https://doi.org/10.1016/j.trpro.2023.02.062
[29] Alzoubi, H.M., Ghazal, T.M., Hasan, M.K., Alketbi, A., Kamran, R., Al-Dmour, N.A., Islam, S. (2022). Cyber security threats on digital banking. In 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, pp. 1-4. https://doi.org/10.1109/ICAIC53980.2022.9896966
[30] Al Hares, A., Zaerinajad, Z., Al Bahr, M. (2024). Customer awareness and cyber security in the organisation for economic co-operation and Development countries. Corporate and Business Strategy Review, 5(1): 371-381. https://doi.org/10.22495/cbsrv5i1siart11
[31] Andriani, Hermantoro, B. (2023). Optimizing financial technology literacy in minimizing phishing threats (case study of indonesian sharia bank customers). Proceeding International Conferences Islam. Philantrophy, 1(1): 38-52. https://doi.org/10.24090/icip.v1i1.302
[32] Vellamy, F., Wijaya, D.A., Gui, A., Ganesan, Y., Shaharudin, M.S., Pitchay, A.A. (2023). Level of awareness of digital banking users on risk and security in Greater Jakarta. In 2023 8th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, pp. 1249-1253. https://doi.org/10.1109/ICBIR57571.2023.10147691
[33] Sahingoz, O.K., BUBEr, E., Kugu, E. (2024). DEPHIDES: Deep learning based phishing detection system. IEEE Access, 12: 8052-8070. https://doi.org/10.1109/ACCESS.2024.3352629
[34] Akinbowale, O.E., Klingelhöfer, H.E., Zerihun, M.F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. Journal Finance Crime, 27(3): 945-958. https://doi.org/10.1108/JFC-03-2020-0037
[35] Muhammad, F.E., Harefa, B. (2023). Pengaturan tindak pidana bagi pelaku penipuan phisning berbasis web. Jurnal USM Law Review, 6(1): 226-241. http://doi.org/10.26623/julr.v6i1.6649
[36] Andhikaputra, R., Tumbel, S.M.A., Vida, J., Gui, A., Karmawan, I.G.M., Ganesan, Y. (2023). User's awareness of personal data leakage in e-commerce application. E3S Web of Conferences, 426: 02063. https://doi.org/10.1051/e3sconf/202342602063
[37] Latifahi, F.N., Mawardi, I., Wardhana, B. (2022). Threat of data theft (phishing) amid the trend of fintech users in the COVID-19 pandemic (study of phishing in Indonesia). Perisai, 6(1): 74-86. https://doi.org/10.21070/perisai.v6i1
[38] Karim, N.A., Khashan, O.A., Kanaker, H., Abdulraheem, W.K., Alshinwan, M., Al-Banna, A.K. (2024). Online banking user authentication methods: A systematic literature review. IEEE Access, 12: 741-757. https://doi.org/10.1109/ACCESS.2023.3346045
[39] Hussein, A.S., Sumiati, S., Hapsari, R., Abu Bakar, J. (2023). Bank 4.0 experiential quality and customer loyalty: A serial mediating role of customer trust and engagement. The TQM Journal, 35(7): 1706-1721. https://doi.org/10.1108/TQM-11-2021-0344
[40] Kapliar, K., Maslova, N., Hnoievyi, V. (2024). Risks of the neobanks' activities in the conditions of the economy digitalization. WSEAS Transactions on Information Science and Applications, 21: 11-22. https://doi.org/10.37394/23209.2024.21.2
[41] Yustianti, S., Roesli, M. (2018). Bank Indonesia policy in the national banking crisis resolution. Yurisdiksi, 11(2): 77-90.
[42] Punithavathi, R., Kowsigan, M., Shanthakumari, R., Zivkovic, M., Bacanin, N., Sarac, M. (2022). Protecting data mobility in cloud networks using metadata security. Computer Systems Science and Engineering, 42(1): 105-120. https://doi.org/10.32604/CSSE.2022.020486
[43] Yuspin, W., Fauzie, A. (2018). The effectiveness of spin off as a breakthrough in promoting Islamic Banking in Indonesia. Journal of Social Sciences Research, 2018(6): 213-216.
[44] Sinaga, P.G.C., Suroso, J.S. (2023). The influence of electronic service quality on digital bank application. Journal of Theoretical and Applied Information Technology, 101(10): 3869-3879.
[45] Rupal, J., Singh, R. (2023). Evaluating the impact of E-banking on customer satisfaction: A comprehensive systematic review. Aibi, Revista de Investigacion Administracion e Ingenierias, 11(3): 115-125. https://doi.org/10.15649/2346030X.3375
[46] Dewi, Y., Suharman, H., Koeswayo, P.S., Tanzil, N.D. (2023). Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. Banks Bank System, 18(4): 44-60. https://doi.org/10.21511/bbs.18(4).2023.05
[47] Angusamy, A., Yee, C.J., Kuppusamy, J. (2022). E-banking: An empirical study on customer satisfaction. Journal System Management Sciences, 12(4): 27-38. https://doi.org/10.33168/JSMS.2022.0402
[48] Singh, K. (2019). Impact of retail banking on customer satisfaction in Delhi. International Journal of Research in Computer Application & Management (IJRCM), 4(9). https://doi.org/10.2139/ssrn.3449942
[49] Firdaus, M.I. (2022). Criticsm analysis of the effectiveness of Indonesia's economic criminal policy in the perspective of Islamic law. JCH (Jurnal Cendekia Hukum), 8(1): 85-102. https://doi.org/10.3376/jch.v8i1.570
[50] Sutarli, A.F., Kurniawan, S. (2023). Peranan pemerintah melalui undang-undang perlindungan data pribadi dalam menanggulangi phising di Indonesia. Innovative: Journal of Social Science Research, 3(2): 4208-4221. https://doi.org/10.31004/innovative.v3i2.760
[51] Sautunnida, L. (2018). Urgensi undang-undang perlindungan data pribadi di indonesia: studi perbandingan hukum inggris dan Malaysia. Kanun Jurnal Ilmu Hukum, 20(2): 369-384. https://doi.org/10.24815/kanun.v20i2.11159
[52] Thomas, J.E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal Business Management, 13(6): 1. https://doi.org/10.5539/ijbm.v13n6p1
[53] Kaya, O., Schildbach, J. (2022). EU Monitor Global Financial Markets Artificial Intelligence in Banking. DB Research Mana. http://www.dbresearch.com, accessed on Apr. 25, 2022.