International Journal of Law and Society

E-ISSN .: 3046-9562
P-ISSN .: 3046-9619

Research Article

Victim Protection in Social Engineering Cybercrime: an Islamic Legal Perspective

Dendy Krisandi [1] *, Abdul Halim [2], Hardi Muhar Sungguh [3]

[1] Jurusan Program Pascasarjana, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
[2] Fakultas Ushuluddin dan Agama, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
[3] Fakultas Syariah, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia

* Corresponding Author: dendykrisandi@gmail.com

Abstract: This research examines Islamic legal protection for victims of social engineering crimes within the context of cybercrime. Social engineering is a form of digital crime that exploits psychological manipulation and trust to obtain personal data, system access, or financial benefits. Such crimes cause not only material losses but also immaterial harm, including psychological trauma, violations of privacy, dignity, and personal security. However, positive legal frameworks tend to prioritize offender punishment, while victim protection and recovery remain insufficiently addressed. This study adopts a qualitative approach with a normative-juridical research design, complemented by limited empirical insights. Data were collected through library research on Islamic legal sources—namely the Qur'an, Hadith, and fiqh jināyah—alongside statutory regulations on cybercrime and selected interviews with legal scholars and practitioners. The analysis employs a descriptive-analytical method grounded in the maqāṣid al-sharīʿah framework, particularly the principles of ḥifẓ al-māl (protection of property), ḥifẓ al-ʻirḍ (protection of dignity), and ḥifẓ al-nafs (protection of life and psychological security). The findings demonstrate that Islamic law provides a robust normative foundation for protecting victims of social engineering crimes. Such protection extends beyond retributive punishment through taʻzīr and emphasizes restorative justice by prioritizing victims' rights restoration, offender accountability, and public welfare. Islamic law is both adaptive and relevant in addressing contemporary cybercrime challenges and may serve as a humanistic, just, and responsive model for victim protection in the digital era.

Keywords: Cybercrime Victims; Islamic Legal Protection; Maqāṣid Al-Sharīʿah; Offender Accountability ; Social Engineering.

Received: January 11, 2026
Revised: January 24, 2026
Accepted: February 15, 2026
Available Online: February 19, 2026
Curr. Ver.: February 19, 2026

1. Introduction

The social, economic, and legal landscapes of today have been profoundly altered by the quick development of information and communication technology (ICT). On a never-before-seen scale, digital platforms enable social engagement, communication, governance, and financial transactions. But at the same time, this change has given rise to new kinds of crime, namely cybercrime. Social engineering, a psychological manipulation technique that preys on human trust rather than technical system flaws, is one of its most advanced forms (Yar, 2013). Social engineering tactics, like phishing, pretexting, and baiting, target cognitive biases and emotional reactions to trick victims into divulging private information or transferring financial assets, in contrast to traditional cyberattacks that mostly rely on hacking tools (Button & Cross, 2017).

DOI : https://doi.org/10.62951/ijls.v3i2.894

Cybercrime has become a major transnational issue that affects states, businesses, and individuals worldwide. One of the crime categories with the highest global growth is cyber-enabled fraud, according to the United Nations Office on Drugs and Crime (UNODC, 2013). The spread of social media platforms, internet banking, and digital services has increased the surface area available for criminal exploitation in numerous jurisdictions, including Indonesia. Due to heightened vulnerabilities brought about by the growing integration of digital infrastructure into both the public and private sectors, cybercrime is now a systemic socio-legal problem rather than just a technical one (Wall, 2007).

The Electronic Information and Transactions Law (Undang-Undang Informasi dan Transaksi Elektronik, or ITE Law) is the main law that regulates cybercrime in Indonesia. It was first passed in 2008 and has since been revised to take into account new improvements in technology. Despite being a major regulatory milestone, the ITE Law's implementation has generated a lot of discussion. Critics contend that legal ambiguity has been created by interpretive uncertainties in several provisions and that enforcement is still uneven. More significantly, the current framework is still primarily offender-oriented, prioritizing criminal penalties while offering few all-encompassing victim protection and compensation measures.

Cybercrime in Indonesia is becoming more severe, as evidenced by recent statistics trends. From roughly 495,000 reported cases in 2020 to an expected 4.5 million events in 2024, incidents have skyrocketed, with social engineering appearing as the most commonly reported modus operandi. This increase is in accordance with the rapid digital shift that occurred during and following the COVID-19 pandemic, which increased consumers' dependence on internet services while also putting them at higher risk. The prevalence of identity theft, data breaches, phishing tactics, and digital financial fraud highlights how crucial psychological manipulation is to modern cybercrime.

Victims of crimes involving social engineering are particularly at risk. They suffer intangible harms in addition to material losses, such as privacy intrusions, harm to their reputation, mental discomfort, and a decreased sense of security. The damage is multifaceted and includes psychological distress and a decline in public confidence in digital ecosystems. However, legal systems frequently fail to offer efficient solutions. Access to justice for victims is hampered by complicated procedures, a lack of digital forensic capabilities, and difficulties with cross-border jurisdiction. Additionally, there is still a lack of public awareness of cyber reporting procedures, which leads to underreporting and little recourse.

The disparity between the flexibility of positive legislation and the quick development of cybercrime emphasizes the necessity for more extensive normative research. Legal solutions must include restorative, preventative, and ethical aspects in addition to penal ones. Islamic law provides a valuable normative resource in this regard. Islamic jurisprudence is a comprehensive legal and moral framework that places a strong emphasis on social duty, fairness (‘adl), and the preservation of human dignity. Even though cybercrime is not specifically addressed in traditional Islamic scriptures, its underlying ideas are flexible enough to handle new types of harm.

An especially pertinent analytical framework is offered by the doctrine of maqasid al-shariah, or the purposes of Islamic law. According to recent research, most notably Auda (2008), maqasid includes the preservation of property, life, faith, intelligence, and ancestry. The protection of property (hifz al-mal) by financial exploitation is intimately linked to social engineering crimes. They also compromise psychological security and personal dignity (hifz al-'ird), both of which are essential to human well-being. Purposive legal reasoning that may adapt traditional standards to contemporary digital environments is thus made possible by the maqasid paradigm.

Through concepts like tadlis (misrepresentation or concealment of faults) and gharar (extreme uncertainty or deception in contractual interactions), classical Islamic jurisprudence also confronts fraudulent activity (Al-Zuhayli, 2011). Although historically applied to commercial transactions, these doctrines share essential characteristics with social engineering: intentional deception, abuse of trust, and unlawful appropriation of property. It is possible to classify digital fraud under well-established jurisprudential categories by using analogical reasoning, or qiyas. Crucially, fraud offenses usually fall within the category of transgressions against individual rights (haqq al-adami), where victim reparation and restitution are given priority.

The focus on victim healing is consistent with restorative justice ideas that are becoming more widely accepted in modern criminology. Restorative approaches prioritize mending harm and reestablishing social equilibrium over vengeance alone (Wall, 2007). Islamic criminal law permits a range of punishments with the goals of social protection, rehabilitation, and deterrent, especially under the discretionary category of ta'zir. This adaptability offers theoretical room for combining ethical accountability with contemporary regulatory frameworks.

This study is innovative because it specifically places victims of social engineering crimes at the heart of an Islamic legal framework. Prior research on cybercrime in Indonesia has mostly focused on the ITE Law's statutory interpretation, offender culpability, and technological aspects. Few have offered an integrative approach that combines Islamic criminal law, legal protection theory, and national regulatory practice, or they have methodically investigated victim protection using maqasid-based analysis. In order to bridge the gap between doctrinal scholarship and actual policy formation, this study prioritizes victims as the main subjects of legal protection.

The report also addresses the pressing need for all-encompassing preventive measures. Victimization risks are increased by inadequate cybersecurity procedures, a lack of digital literacy, and a lack of institutional resources. Islamic legal theory can support preventive frameworks that supplement formal regulation because of its emphasis on moral teaching and collective responsibility. Islamic-based accountability systems, social awareness initiatives, and preventive ethics may increase society's resistance against deception.

Critical theoretical concerns are also brought up by the growing complexity of social engineering: Is it possible for Islamic law to properly adjust to the swift advancements in technology? How could modern cyber governance frameworks operationalize the traditional concepts of justice and compensation? It takes an interdisciplinary approach involving criminological theory, cyber law, and Islamic jurisprudence to address these issues. In addition to enhancing Islamic legal studies, this kind of interaction advances the worldwide conversation on culturally sensitive cybercrime legislation.

In the end, a multifaceted legal response is required to safeguard victims of social engineering crimes. Although positive law offers crucial regulatory underpinnings, its shortcomings in guaranteeing restorative justice necessitate the use of supplementary normative resources. Islamic law provides a framework that is both morally sound and flexible, as it is based on universal values of justice and human dignity. A more humanistic and adaptable model of cyber victim protection might be created by combining restorative justice orientation, fraud doctrines, and maqasid-based reasoning.

Therefore, the goal of this research is to develop an Islamic legal framework that is both doctrinally sound, practically applicable, and sensitive to Indonesia's modern digital reality in order to safeguard victims of social engineering cybercrime. By doing this, it makes a theoretical contribution to the evolution of modern Islamic legal theory as well as a practical one to the policy discussion around victim-centered cybercrime governance. In principle, it is part of a policy that is understood as an action taken by the government to overcome a problem (HM *et al.*, 2026).

2. Literature Review

The study of cybercrime theory looks at illegal activity carried out using information technology and digital networks. Hacking, identity theft, online fraud, data breaches, illegal interception, ransomware attacks, and the distribution of damaging or illegal content are all considered forms of cybercrime (Wall, 2007). Social engineering, which depends on psychological manipulation rather than just technical infiltration, is one of the most used techniques in modern digital environments. To collect sensitive data or gain illegal access to systems, criminals take advantage of human trust, cognitive bias, and a lack of cybersecurity awareness (Hadnagy, 2018). Cybercrime is more complex to detect and enforce than traditional crimes because of its anonymity, speed, automation, and multinational reach (Brenner, 2010).

Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was most recently revised by Law No. 1 of 2024, governs cybercrime in Indonesia. Illegal access (hacking), unlawful interception, data manipulation, identity theft, online defamation, and the spread of false information are all prohibited by the statute. Despite its significance, there are still issues with enforcement, such as unclear interpretations, a lack of technical expertise among law enforcement organizations, and quick technological advancements that frequently surpass regulations (Susanto, 2022). From the standpoint of Islamic criminal law, such statutory regulations can be interpreted in the context of taʿzīr, which gives state authorities the authority to decide on suitable punishments for crimes that aren't specifically mentioned in primary sources as long as they promote the general welfare (maṣlaḥah) (Kamali, 2008).

The main focus of legal protection theory is on how legal systems guarantee victims' rights and justice. Protection include restitution, reparation, procedural justice, and psychological healing in addition to punishing perpetrators (Ashworth, 2014). Victims of cybercrime frequently experience both immaterial costs, such as psychological discomfort, privacy intrusions, and reputational damage, as well as tangible losses, such as financial theft. Therefore, victim-centered processes, accessible reporting platforms, reparation mechanisms, and digital forensic assistance are necessary for effective legal protection (UNODC, 2013).

However, victim protection is sometimes hampered by implementation deficiencies. When pursuing remedies, many victims are unaware of their rights or encounter complicated procedures. Cross-border cybercrime also makes coordination of enforcement and jurisdictional authority more difficult. Therefore, in addition to statutory clarity, comprehensive protection necessitates international collaboration, institutional capacity-building, and digital literacy programs.

Cohen and Felson (1979) developed Routine Activity Theory (RAT), which offers a situational framework for comprehending cybercrime. According to the hypothesis, crime happens when three factors come together: a suitable target, a motivated perpetrator, and the lack of a skilled guardian. Hackers and fraudsters who are driven by money, ideology, or reputational recognition are examples of cybercriminals. Vulnerable digital assets, such as unprotected systems, financial data, or accounts with inadequate security, make good targets. Inadequate cybersecurity safeguards, lax regulatory monitoring, or low user awareness are all examples of the lack of skilled guardians.

Because online environments constantly create opportunities for offenders and targets to converge, RAT is especially pertinent in digital circumstances. Inadequate system updates, phishing vulnerability, and weak passwords decrease guardianship, which raises the danger of victimization. RAT-derived crime prevention tactics emphasize lowering target suitability (e.g., data minimization and multi-factor authentication), boosting deterrence through efficient enforcement, and fortifying digital guardianship (e.g., encryption, firewalls, intrusion detection systems) (Leukfeldt & Yar, 2016).

To sum up, legal protection theory stresses victim-centered justice, routine activity theory reveals the situational dynamics that facilitate cybercrime, and cybercrime theory analyzes the changing technological and psychological mechanics of digital offending. When combined, these frameworks offer a thorough analytical basis for combating cybercrime via victim protection, prevention, and legislation.

3. Method

A normative (doctrinal) legal research design with a qualitative focus is used in this study. All primary materials for this library-based investigation come from reliable textual sources, such as academic monographs, statutory regulations, peer-reviewed journal articles about cybercrime, social engineering, and victim protection, as well as classical and modern Islamic legal literature. As opposed to empirical measurement (IRAC-based doctrinal technique), normative legal research concentrates on the examination of legal principles, doctrines, and conceptual frameworks (Hutchinson, 2018). Therefore, in the context of cybercrime legislation, this study looks at how Islamic law conceptualizes the protection of victims of social engineering crimes.

In order to systematically explain the legal characteristics of social engineering as a cyber offense and to examine the degree to which Islamic legal principles—specifically, maqāṣid al-sharīʿah—provide normative foundations for victim protection, the study employs a descriptive-analytical approach (Kamali, 2008). The goal is to create an optimal and flexible legal protection model based on Islamic criminal jurisprudence (fiqh jināyah), not to scientifically assess law enforcement performance. Contextual information on the rise in cybercrime is not an actual variable; rather, it is merely background justification.

The relationship between Islamic legal concepts and Indonesian positive law—specifically, Law No. 11 of 2008 on Electronic Information and Transactions as modified by Law No. 1 of 2024—is also evaluated using a comparative method. The discovery of normative convergence and variance between national cybercrime regulations and Islamic law is made possible by comparative legal analysis (Zweigert & Kötz, 1998). This approach aids in the development of comprehensive policy suggestions meant to reinforce victim-centered legal change.

The Qur'an, Hadith, traditional fiqh treatises, current Islamic legal scholarship, statutory instruments, court rulings, and international studies on cybercrime are among the primary secondary legal documents that the research uses as data sources. To improve conceptual clarity, scholarly conversations about social engineering and digital victimization are also included (Wall, 2007; Hadnagy, 2018). In order to extract normative principles pertinent to victim rights, state responsibility, and justice restoration, these materials undergo qualitative examination using content analysis and doctrinal interpretation.

Finding fundamental Islamic legal concepts pertaining to the defense of property (ḥifẓ al-māl), dignity (ḥifẓ al-ʿirḍ), and security (ḥifẓ al-nafs) and combining them with current cybercrime standards constitute the analytical process. The paper creates a thorough model of Islamic legal protection that takes into account victim rehabilitation, accountability, and prevention in digital situations using methodical legal reasoning. Finally, this normative-conceptual framework advances the discourse on protecting victims of cybercrime in both state law policy and Islamic jurisprudence.

4. Results and Discussion

Social Engineering in Cybercrime: Forms, Victim Characteristics, and Multidimensional Harm

One of the most prevalent types of modern cybercrime is social engineering, which is identified by its dependence on psychological manipulation as opposed to only technical exploitation. Social engineering uses human cognition, trust, emotion, and behavioral bias as the main attack surface, in contrast to traditional hacking, which focuses on software flaws or network weaknesses (Hadnagy, 2018; Mitnick & Simon, 2011). Social engineering has become a primary means of cyber victimization in increasingly digitalized society where communication, identity verification, and financial transactions take place online. The manipulation of trust, urgency, anxiety, empathy, and habitual digital habits is what makes it so powerful, especially in settings with a high reliance on digital services and little cybersecurity knowledge (Wall, 2007).

The most common form of social engineering is still phishing. It entails misleading electronic communications—through social media, instant messaging, SMS (smishing), or email—that are intended to trick victims into disclosing private information like passwords, banking login credentials, or one-time authentication codes. Phishing's primary tactic is not technological expertise but rather manipulation of trust, which is often maintained by impersonating trustworthy organizations and using emotional cues like fear or urgency (Hadnagy, 2018). Phishing is frequently cited in empirical cybersecurity surveys as the main way that financial fraud and data breaches occur (Verizon, 2023). Attack success rates are raised by variations like spear-phishing and whaling, which further customize attacks.

Pretexting is a more focused tactic used by criminals to convince victims that they have legitimate power by creating complex false scenarios. Criminals may pose as bank employees, public servants, or law enforcement personnel, frequently bolstering their credibility with personal information gleaned from public sources or prior security breaches. Pretexting, in contrast to mass phishing efforts, is narrative-driven and contextual, taking advantage of societal presumptions regarding the legitimacy and authority of institutions (Mitnick & Simon, 2011). From a criminological standpoint, this method uses digital interactions to weaponize symbolic power and social hierarchy.

Baiting works by promising rewards, including investment earnings, social aid, or promotional benefits, to pique victims' interest or fulfill their financial ambitions. Baiting takes advantage of hope and perceived opportunity instead of fear. In an attempt to obtain the promised benefit, victims can send money, download harmful software, or divulge personal information. Economic weakness and financial incentives have been shown to dramatically increase vulnerability to such methods (Leukfeldt, 2014). Baiting frequently combines psychological manipulation with the deployment of technical malware, illustrating the hybrid character of contemporary cybercrime.

The field of social engineering is further broadened by impersonation and manipulation on social media. While manipulation may involve the planned distribution of false information to sway perception and affect action, impersonation is the construction of false digital identities that mirror real people or organizations. By creating the appearance of social evidence and legitimacy, social media platforms' interactive and algorithm-driven design increases the legitimacy of such attacks (Wall, 2007). These tactics show how cybercrime is moving away from system-based exploitation and toward relational exploitation.

The majority of social engineering strategies are based on emotional engineering, which uses fake empathy, urgency, and terror. Criminals purposefully cause fear or cognitive overload to impair victims' ability to verify information rationally. Stress and time pressure have been shown in psychological studies to dramatically impair important decision-making, leading to what behavioral scholars refer to as constrained rationality (Kahneman, 2011). As such, victims' acts are responses influenced by manipulative cues rather than totally autonomous or informed consent.

In contrast to victims of traditional crimes, victims of social engineering are more vulnerable due to their cognitive and psychological vulnerabilities rather than their physical frailty or lack of technological knowledge. Exposure to manipulation is increased by regular online involvement, response to digital notifications, and high levels of institutional trust (Leukfeldt, 2014). Crucially, victims are not limited to particular demographic categories; people with high levels of education or occupation may be singled out by narratives that are specifically tailored to their social responsibilities.

Vulnerability is further increased by poor data security procedures and low levels of digital literacy. Beyond technical competence, digital literacy encompasses critical assessment of online communication and knowledge of cybersecurity threats (OECD, 2020). Human-centric cyberattacks are successful because of poor password management, a lack of multi-factor authentication, and a lack of awareness about the need of data protection (Verizon, 2023). The literature on victimology, however, warns against characterizing such weaknesses as carelessness. Rather, they reflect structural deficiencies in institutional safeguards and digital education. Additionally, reliance on digital services like social media, e-commerce, and online banking increases risk exposure. Regular engagement with digital alerts normalizes quick reactions and encourages automation bias, in which people uncritically accept signals supplied by the system (Kahneman, 2011). By including fraudulent communication into anticipated service flows, criminals take advantage of these behavioral tendencies.

Social engineering victims should be viewed as unintentional victims from a victimological perspective. They do not actively engage in wrongdoing and lack mens rea; instead, they are the victims of psychological coercion and misleading consent produced by informational asymmetry. According to Leukfeldt (2014), victim-blaming narratives conceal the structural and cognitive manipulation that these crimes entail. This is highlighted by contemporary cyber-victimology. Creating victim-centered justice frameworks requires acknowledging victims as unintentional participants.

Social engineering causes harm that is multifaceted. The most obvious result is material loss, such as money stolen, accounts compromised, or digital assets taken. Research continuously shows that a significant amount of worldwide cybercrime costs are attributable to fraud based on social engineering (Verizon, 2023). Identity theft, improper credit applications, and long-term economic instability are examples of financial harm that goes beyond immediate loss. However, immaterial harm is frequently more severe. Psychological stress, anxiety, shame, and low self-esteem are common among victims. According to research on cyber-victimology, victims of digital fraud show stress reactions similar to those of victims of more conventional crimes, especially when their financial security is at risk (Leukfeldt, 2014). Underestimation of the occurrence persists because reporting is discouraged by shame and fear of stigma.

Another important aspect of injury is the loss of honor and privacy. Autonomy and dignity are undermined by unauthorized access to personal data, and social reputation can be harmed by improper use of compromised accounts. Privacy violations have relational and emotional repercussions in digital cultures as social contact and identity are mediated online (Wall, 2007). All of these negative effects highlight the fact that social engineering is a breach of psychological integrity and human dignity in addition to being a financial crime. Therefore, a victim-centered strategy that incorporates reparations, psychological assistance, the advancement of digital literacy, and structural change of cybersecurity governance is necessary for effective legal and regulatory responses.

Victim Protection in Social Engineering Crimes under Indonesian Positive Law

Protection for victims of social engineering cybercrimes is still fundamentally limited and primarily offender-oriented under Indonesian positive law. The main legislative framework, Law No. 11 of 2008 on Electronic Information and Transactions as revised by Law No. 1 of 2024 (ITE Law), was not intended to create a complete victim protection regime, but rather to prosecute forbidden conduct in cyberspace. Its normative design reflects a punitive or retributive attitude by defining transgressions, establishing components of responsibility, and prescribing penal sanctions (Muladi & Arief, 2010).

Social engineering victims are not specifically acknowledged as independent legal persons with certain rights under this framework. Rather, they manifest implicitly as "injured parties," whose losses are used as supporting evidence for criminal aspects. As a result, victims are usually framed as witnesses or proof rather than as actors with rights to compensation, rehabilitation, or restoration of their online reputation. This structure demonstrates how Indonesian cyber law continues to adhere to an offender-centered justice paradigm.

The ITE Law's lack of specific measures for restitution, compensation, psychological support, or post-crime digital recovery further demonstrates normative limitations. While the Witness and Victim Protection Agency (LPSK) offers procedures for protection and compensation under Law No. 31 of 2014 amending Law No. 13 of 2006 on Witness and Victim Protection, its application in cybercrime cases is still selective and dispersed. Victims of non-physical cyber fraud do not automatically have access to structured recovery mechanisms because the regime was originally created to combat violent and significant conventional crimes (LPSK, 2022). Because of this, victims frequently have to file a second civil lawsuit in order to recover damages, which adds to their financial and emotional burdens.

Additionally, protection is dispersed and indirect. Without a cohesive, victim-centered framework for cybercrime, victim-related protections are scattered throughout the ITE Law, the Criminal Procedure Code (KUHAP), and the Witness and Victim Protection Law. Legal ambiguity is brought about by fragmentation, which also leaves protection mostly up to the judgment of law enforcement. According to contemporary victimology, these structural flaws lead to underreporting and a decline in confidence in criminal justice systems (UNODC, 2013).

The most official kind of protection is the reporting and law enforcement system. In order to start an inquiry and prosecution, victims can report events to law enforcement, including cybercrime units. However, rather than rehabilitating victims, the main goal of this mechanism is to punish criminals. Proceedings are frequently drawn out and technical because to complex evidentiary requirements, such as cross-border collaboration and digital forensic verification. Often without expert help, victims are required to complete procedural formalities and submit electronic proof. This may result in secondary victimization, in which psychological anguish is made worse by the legal system itself (Doerner & Lab, 2018).

Another useful, if mostly technological, type of protection is post-crime account and data security procedures. It is advised that victims update their passwords, turn on multi-factor authentication, and work with online platforms or financial institutions to freeze their accounts. Although these steps prevent additional harm, they are not routinely governed by the ITE framework and rely mostly on the digital literacy of the victims as well as platform-specific regulations. The likelihood of recurrent victimization rises in the absence of established state-backed healing processes.

The lack of organized compensatory and psychological rehabilitation programs is a significant gap. In addition to monetary loss, social engineering crimes cause anxiety, damage to one's reputation, and a decline in trust. However, compensation is not required by Indonesian internet law as a fundamental part of criminal punishment. Victims are disproportionately burdened in the absence of formalized recovery procedures, which compromises substantive justice and erodes public trust in cyber law enforcement.

The lack of a victim-centered approach is revealed by the accumulation of these shortcomings. According to modern criminal justice theory, victim restoration and offender accountability must be integrated (Muladi & Arief, 2010). A solely punitive strategy is normatively insufficient in the case of manipulative cybercrimes, when victims are unintentional agents who are subjected to psychological manipulation. Therefore, reform is needed to incorporate digital reputation recovery, psychological rehabilitation, restitution, and streamlined reporting procedures into Indonesia's cybercrime framework. Victim protection in social engineering instances will continue to be formalistic, disjointed, and substantively lacking in the absence of such a paradigm shift.

Social Engineering as Taḥrīm and Taʿzīr in Islamic Criminal Law: A Maqāṣid-Based Victim Protection Framework

Despite being mediated by technology, social engineering is a modern form of fraud that is normatively equivalent to traditional Islamic legal prohibitions. In order to persuade victims to give up assets, information, or the ability to make their own decisions, it entails deliberate manipulation, information fabrication, truth hiding, and trust exploitation. Such behavior is considered a banned act (taḥrīm) in Islamic jurisprudence since it violates amānah (trust), gharar (deceptive uncertainty), tadlīs (fraudulent misrepresentation), and unjust enrichment (akl al-māl bi al-bāṭil). Despite being digital, the legal content is similar to traditional fraud that is prohibited by fiqh al-muʿāmalāt (Al-Zuḥailī, 2011; Ibn Taymiyyah, 1998).

According to Al-Zuḥailī (2011), gharar is defined as excessive ambiguity or intentional obscurity that compromises informed agreement and results in unjust injury in Islamic economic jurisprudence. Social engineering purposefully creates informational asymmetry in order to replicate this system. Victims are denied correct information about the identity, intent, or repercussions of the desired action of the perpetrator. Because it undermines transactional justice and invalidates genuine consent (riḍā), traditional jurists unequivocally forbid gharar fāḥish (grave deception), which is what this contrived ambiguity is (Ibn Rushd, 2004).

Tadlīs, the deliberate concealment of flaws or fabrication of important information in order to gain consent, is closely linked. Cybercriminals create fake digital interfaces, alter narratives, and pose as trustworthy organizations in order to mimic authenticity. Since permission based on false grounds is invalid under Islamic law, such behavior eliminates true volition (Al-Zuḥailī, 2011). As a result, any transfer of assets or information acquired by deception cannot be considered legally binding; the offender bears full responsibility.

A fundamental normative basis for classifying social engineering as ḥarām is established by the Prophetic condemnation of deceit ("Whoever deceives us is not of us") and the Qur'anic prohibition against devouring property wrongfully (Qur'an 4:29). The fundamental moral wrong—willful manipulation of the truth for illegal gain—has not changed, despite the medium's evolution. Social engineering is a psychological violation that goes beyond economic harm since it interferes with reasonable thought and judgment. Protection of intellect (ḥifẓ al-ʿaql) is one of the five fundamental goals of the maqāṣid al-sharīʿah framework (Al-Ghazālī, 1993; Auda, 2008). Islamic law views moral obligation (taklīf) as rooted in the intellect. A protected value is compromised by any intentional attempt to impede rational decision-making, whether by force, intoxication, or deceit.

Social engineering uses emotional coercion, cognitive manipulation, and the exploitation of trust biases. As a result, the impact goes beyond monetary loss to include the loss of psychological stability and autonomy. According to maqāṣid, this is a compound offense as it harms both ḥifẓ al-ʿaql and ḥifẓ al-māl. Deception also implicates ḥifẓ al-ʿirḍ (defense of honor) when it leads to identity misuse or reputational injury. Therefore, the offense violates several protected interests at the same time, which increases its seriousness according to Islamic law (Auda, 2008). Non-physical injury is acknowledged as legally significant by Islamic jurisprudence. Rafʿ al-ḍarar, the idea of eradicating harm, emphasizes that harm encompasses more than just physical harm; it also covers psychological and reputational suffering. Social engineering victims are therefore categorized as maẓlūm (wronged parties), and their consent—obtained through deceit—has no legal significance.

Sincerity (ṣidq) and trust (amānah) are the moral cornerstones of Islamic social order. Both are undermined by social engineering, which uses trust as a tool for exploitation. Because informational integrity is essential to social cohesion, classical jurists view betrayal of trust (khiyānat al-amānah) as a grave moral and legal transgression (Ibn Taymiyyah, 1998). The extent of such betrayal is exacerbated in the digital sphere, where identity manipulation and impersonation undermine public trust in institutions and interpersonal interactions. According to maqāṣid, systemic fasād (social corruption) is caused by the breakdown of trust. Therefore, the offense goes beyond individual victimization to cause injury to the entire community, which justifies state action under the public interest doctrine (maṣlaḥah).

Crimes are categorized as ḥudūd, qiṣāṣ–diyāt, or taʿzīr in fiqh jināyah. Social engineering is classified as jarīmah taʿzīr, or offenses whose punishment is discretionary and decided by a legitimate authority, as it does not have a precise textual penalty in the Qur'an or Sunnah (Ibn Taymiyyah, 1998). The flexibility of Islamic criminal law is demonstrated by the lack of express nash, which does not entail normative silence. Deterrence (zajr), reformation (iṣlāḥ), and public welfare protection are the goals of taʿzīr. Flexibility in sanctions is crucial since social engineering can range from solitary fraud to coordinated cyber manipulation. Judges can adjust the severity of punishment based on the victims' vulnerability, the extent of the injury, the intentionality, and the social consequences. The maxim that states that a court's decision should be in line with its effective cause (al-ḥukm yadūru maʿa ʿillatihi) is in line with this proportionality concept (Kamali, 2008). If they serve maqāṣid-oriented goals, potential sanctions could include monetary compensation, incarceration, digital limitations, or rehabilitation efforts. Ta'zīr's discretionary character guarantees adaptability to technical advancement without sacrificing doctrinal integrity.

In taʿzīr punishment, Islamic legal doctrine places a strong emphasis on proportionality. Material loss, psychological anguish, reputational harm, and the breakdown of social trust are all considered forms of harm (ḍarar). More severe punishment is appropriate for more harm. More severe punishments are justified for coordinated schemes that impact numerous victims as opposed to isolated incidents. Rather than strict formality, this graded approach expresses genuine justice.

Crucially, proportionality incorporates healing components as well. Restitution and compensation represent the Qur'anic devotion to justice and equity and serve both punitive and reparative purposes. Islamic criminal law, thus, allows for a restorative justice perspective that aligns with modern victim-centered methodologies. Islamic law's flexibility stems from its maqāṣid-based approach. The law continues to have normative relevance for non-physical cyber offenses by assessing harms based on protected values rather than historical forms. Despite being a new technology, social engineering is a modern take on traditional dishonesty.

Islamic law exhibits conceptual flexibility and ethical continuity through the taʿzīr mechanism and maqāṣid analysis (Auda, 2008; Kamali, 2008).

According to Islamic law, social engineering is a criminal offense under jarīmah taʿzīr and a prohibited conduct (taḥrīm). It violates the maqāṣid protections of intellect, property, and honor while also incorporating gharar, tadlīs, breach of amānah, and unjust enrichment. Ta'zīr's discretionary framework permits context-sensitive, proportionate sanctions that are in line with victim restitution and deterrence. Islamic criminal jurisprudence is far from being out of date; rather, it provides a logical and flexible normative framework that can deal with contemporary cyber deceit while maintaining societal welfare, justice, and human dignity.

Comparison

The novelty of this research lies in the formulation of Islamic legal protection for victims of criminal acts of social engineering (social engineering) in cyber crimes which places the victim as the main subject of legal protection, not just a complement to the punishment of the perpetrator. Different from previous studies which tend to focus on the technical aspects of cyber crime or normative analysis of positive law, this research develops the construction of contemporary fiqh jināyah by positioning social engineering as a digital-psychic crime that has a direct impact on maqāṣid al-sharīʿah violations, especially ḥifẓ al-māl, ḥifẓ al-ʿirḍ, and ḥifẓ al-nafs.

By extending the interpretation of taʿzīr beyond traditional physical or transactional crimes to include cognitive and psychological manipulation in digital environments, the work theoretically enhances Islamic legal theory. It supports the claim that, as opposed to strict textual formalism, Islamic criminal law functions through value-based reasoning. Furthermore, the research supports the methodological soundness of maqāṣid as a dynamic tool for modern legal reform by establishing cyber deception in well-established jurisprudential principles rather than relying solely on analogical approximation.

In practice, the results offer normative recommendations for judges, legislators, and Islamic legal experts in Muslim-majority countries dealing with cybercrime. Proportional sentencing, restitution-centered remedies, and preventive regulation in line with the public interest (maṣlaḥah) are all made possible by the taʿzīr framework. In order to improve doctrinal consistency and institutional responsiveness in the digital age, the study also advocates for the incorporation of Islamic legal concepts into victim compensation plans, cybercrime laws, and digital ethics education.

6. Conclusion

Social engineering in cyber crime, according to the perspective of Islamic law, is a form of crime based on psychological manipulation which is contrary to the principles of honesty, trustworthiness and the prohibition of fraud (tadlīs and gharar). Even though there is no explicit regulation in the Al-Qur'an and hadith regarding cyber crimes, Islamic law through the maqāṣid al-sharī'ah approach is able to construct social engineering as an act of mischief because it clearly violates the protection of property (ḥifẓ al-māl), honor and privacy (ḥifẓ al-'irḍ), as well as the victim's sense of security and psychological condition (ḥifẓ al-nafs). Thus, social engineering is positioned as a non-physical crime that has serious impacts and is relevant to be categorized within the framework of contemporary fiqh jināyah. Islamic law's form of protection for victims of criminal acts of social engineering is not limited to the aspect of punishing the perpetrator, but includes comprehensive protection that is preventive, repressive and restorative. Islamic law offers a protection mechanism through the concept of ta'zīr as the basis for the legitimacy of adaptive sanctions, while emphasizing the restoration of victims' rights through compensation, psychological rehabilitation, and restoration of social dignity. This approach shows the superiority of Islamic law which is not only oriented towards legal certainty, but also towards substantive justice and benefit, so that victims of cyber crime are positioned as the main subject of legal protection, not just a means of proof in the judicial process.

Author Contributions: Conceptualization: Dendy Krisandi and Abdul Halim; Methodology: Wiji Nur Eko Wahyu and Hardi Muhar Sungguh; Validation: Dendy Krisandi and Abdul Halim; Formal analysis: Dendy Krisandi and Hardi Muhar Sungguh; Investigation: Dendy Krisandi and Abdul Halim; Resources: Dendy Krisandi and Abdul Halim; Data curation: Dendy Krisandi and Abdul Halim; Writing—original draft preparation: Dendy Krisandi; Writing—review and editing: Dendy Krisandi; Visualization: Dendy Krisandi and Hardi Muhar Sungguh; Supervision: Abdul Halim.

Funding: This research received no external funding.

Data Availability Statement: Complete data from this research was found in the Postgraduate Program of UIN Sulthan Thaha Saifuddin, Jambi.

Acknowledgments: We would like to thank the Postgraduate Program, UIN Sulthan Thaha Saifuddin for providing both material and non-material facilities for supporting this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

Al-Ghazālī. (1993). *Al-Mustaṣfā min 'ilm al-uṣūl*. Dār al-Kutub al-'Ilmiyyah.

Al-Zuḥailī, W. (2011). *Al-fiqh al-islāmī wa adillatuhu*. Dār al-Fikr.

Ashworth, A. (2014). *Positive obligations in criminal law*. Hart Publishing.

Auda, J. (2008). *Maqasid al-shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought. https://doi.org/10.2307/j.ctvkc67tg

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger. https://doi.org/10.5040/9798400636554

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge. https://doi.org/10.4324/9781315679877

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Doerner, W. G., & Lab, S. P. (2018). *Victimology* (8th ed.). Routledge. https://doi.org/10.4324/9781315537054

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley. https://doi.org/10.1002/9781119433729

HM, Pahrudin, & Hatta Abdi Muhammad, Burlian Senjaya, Samia Elviria, Zakly Hanafi Ahmad, Syafrial, Salman. (2026). The Study of Local Government Policy and its Impact on Public Satisfaction and Incumbent Electability: An Analysis of Experiences from Jambi Province. *Jurnal Public Policy, Vol 12, No 1* (2026), DOI: https://doi.org/10.35308/jpp.v12i1.11702.

Hutchinson, T. (2018). *Researching and writing in law* (4th ed.). Thomson Reuters.

Ibn Rushd. (2004). *Bidāyat al-mujtahid wa nihāyat al-muqtaṣid*. Dār al-Ḥadīth.

Ibn Taymiyyah. (1998). *Al-Siyāsah al-shar'iyyah fī iṣlāḥ al-rā'ī wa al-ra'iyyah*. Dār al-Kutub al-'Ilmiyyah.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kamali, M. H. (2008). *Shari'ah law: An introduction*. Oneworld Publications.

Lembaga Perlindungan Saksi dan Korban (LPSK). (2022). *Annual report*. LPSK.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime. *European Journal of Criminology, 13*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley.

Muladi, & Arief, B. N. (2010). *Teori-teori dan kebijakan pidana*. Alumni.

OECD. (2020). *Digital security risk management: A strategic approach*. OECD Publishing.

Susanto, H. (2022). Cyber law enforcement challenges in Indonesia. *Journal of Indonesian Legal Studies, 7*(2), 145-162.

United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive study on cybercrime*. United Nations.

Verizon. (2023). *2023 data breach investigations report*. Verizon Enterprise.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.

Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (3rd ed.). Oxford University Press.