LEGAL RESPONSES TO PHISHING FRAUD IN INDIA: AN ANALYSIS ON THE EMERGING CHALLENGES IN CYBER JURISPRUDENCE

Trisha M V, School of Law, CHRIST (Deemed to be University)

ABSTRACT

Cyber jurisprudence is the study of law related to computer-related crimes. Cybercrimes are of three types - crime against individuals, property and government. My article focuses on cybercrime against property which involves phishing fraud. Additionally, the role of AI adds fuel to the fire of phishing fraud. Phishing fraud has become a serious cyber threat in India due to the rapid growth of digital banking and online financial transactions. Fraudsters use fake emails, messages, and websites to trick people into sharing sensitive information such as OTPs, passwords, and bank details, which are then used for unauthorized financial transfers. Although such acts are increasing in number, phishing is not specifically recognized as an independent offence under Indian cyber law. At present, these offences are dealt with under general provisions relating to cheating, impersonation, and identity theft, which creates difficulty in proper investigation, legal classification, and enforcement.

This paper analyses the existing legal responses to phishing fraud in India and examines the emerging challenges faced within the framework of cyber jurisprudence. It discusses issues such as lack of specific legislation, evidentiary challenges in digital crimes, and delays in securing remedies for victims. The study further highlights the need for legal reform, including the recognition of phishing as a separate cyber offence and the use of technological tools such as artificial intelligence for early detection of fraudulent activities. The objective of this paper is to evaluate the adequacy of the present legal framework and suggest necessary reforms to strengthen the protection available to victims of phishing fraud in India.

Keywords: Phishing Fraud, Cybercrime, Cyber Jurisprudence, Information Technology Act, Digital Fraud, Artificial Intelligence.

I. Introduction

The concept of the Digital Economy, first introduced by Don Tapscott in his book *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, refers to an economic system driven by digital computing technologies and internet-based information infrastructure.[1] Financial frauds such as phishing and vishing have become increasingly common with the rise of digital banking and online transactions in India[2]. Phishing generally involves tricking individuals into clicking malicious links or entering sensitive financial information on fake websites or applications that appear to belong to legitimate institutions such as banks. Vishing adds another layer to such frauds by using voice calls to build trust and manipulate victims into sharing confidential information or downloading malicious applications. These attacks often rely on social engineering techniques, where fraudsters create a sense of urgency by claiming that bank accounts, cards, or reward points are about to expire.

Phishing and vishing attacks are non-violent cybercrimes that do not cause physical harm but result in financial loss, psychological distress, and social damage[3]. These offences heavily rely on anonymity and technological manipulation. Fraudsters use techniques such as caller ID spoofing, masked IP addresses, fake domain names, and encrypted communication channels to conceal their identity[4]. The use of such methods not only complicates the process of tracing the accused but also challenges existing legal frameworks that were originally designed to deal with identifiable offenders in physical spaces.

II. Defining Phishing

According to the Oxford English Dictionary, "phishing" refers to fraudulent practice in which emails are sent pretending to be from trusted organizations, with the intention of tricking individuals into disclosing sensitive personal details such as passwords, banking credentials, or credit card information through online platforms. Phishing methods are carried out through various modes such as spam emails, voice calls (vishing), highly targeted attacks like spear phishing and whaling, fraudulent SMS messages (smishing), QR code-based scams (quishing),

[1] Dr. Devendra Jarwal, *Digital Economy & India*, SSRN (Jun. 24, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3405961
[2] Justice SR Krishna Kumar and Jay Vijayan, *The Rise of AI-Powered Cybercrime: India's Threat & Mitigation Report 2025*, GIREM 25, 6-59 (2025).
[3] Vishi Aggarwal and Ms. Shruti, *Cybercrime Victims: A Comprehensive Study*, 6(2) IJCRT 643, 640-648 (2018).
[4] KEVVIE FOWLER, DATA BREACH PREPARATION AND RESPONSE 1-26 (Syngress 2016).

and man-in-the-middle attacks aimed at bypassing two-factor authentication. Email phishing is the most widespread form, where fraudulent messages are sent in bulk to a large number of users, directing them to fake login pages in order to obtain sensitive details such as passwords or banking information.[5] The stolen data may be used for financial theft, spreading malware, or carrying out further targeted attacks. In vishing or voice phishing attacks, criminals use Voice over Internet Protocol (VoIP)[6] technology to place automated calls to a large number of people, often with the help of text-to-speech systems, falsely informing them about suspicious activity in their accounts. They manipulate the caller ID so that the call appears to originate from a genuine bank or institution. The person receiving the call is then asked to share confidential details or is connected to an operator who tries to extract such information through deceptive communication methods.

According to Kevin Mitnick, "social engineering" refers to a subset of con-artistry where a person "uses deception, influence, and persuasion against businesses, usually targeting their information"[7]. Attackers often create a fabricated narrative to justify the demand for confidential information. For example, individuals may be informed that their bank account will be frozen unless immediate verification is completed, or that they are entitled to a monetary reward subject to the disclosure of account details for processing purposes. Social engineering methods rely on weaknesses in human judgment and perception, commonly referred to as cognitive biases[8], which can be easily manipulated. On the other hand, identity theft, also referred to as identity infringement, takes place when a person unlawfully uses another individual's personal details such as their name, identification number, or credit card information to carry out fraud or other illegal acts. Establishing a clear connection between data breaches and incidents of identity theft is difficult, as victims are usually unaware of how their personal information was accessed. As noted in a report prepared for the Federal Trade Commission (FTC)[9], offences involving phishing often go unnoticed by the affected individuals. While identity fraud frequently results from identity theft, it is not an inevitable outcome in every case.

[5] Steven Furnell et al., *Fifteen years of phishing: Can Technology save us?* 7 Computer Fraud & Security, 11-16 (2019).
[6] Slade E. Griffin and Casey C. Rackley, *Vishing*, Proceedings of the 5th Annual Conference on Information Security Curriculum Development 35, 33-35 (2008).
[7] KEVIN F. STEINMETZ ET AL., CRITICAL CRIMINOLOGY 632 (Springer 2020).
[8] Baris Kirdemir, *Hostile Influence And Emerging Cognitive Threats In Cyberspace*, Centre for Economics and Foreign Policy Studies 13, 1-16 (2019).
[9] Federal Trade Commission – 2006 Identity Theft Survey Report, Synovate 4, 1-108 (2007).

Phishing is not confined by geographical limits. The borderless nature of the internet poses significant challenges for law enforcement agencies in tracking and prosecuting cybercriminals[10]. For example, an offender may operate from one country, target victims in another country, and transfer stolen funds through accounts located in several other jurisdictions. This cross-territorial element complicates investigation and prosecution because it requires cooperation between multiple legal systems, each having its own procedural laws and data-sharing restrictions.

Offenders frequently hide their identities by using encrypted communication tools, proxy servers, or false digital credentials. The use of fake accounts, virtual identities, and layered financial transactions make it difficult to trace the real individual behind the offence. Money mule networks further complicate identification, as funds are transferred through several intermediaries before reaching the final beneficiary, thereby distancing the offender from the original act of fraud[11]. In few circumstances involving cyber financial crimes, most of the evidence exists in electronic form, such as transaction logs, IP addresses, email records, or server data. Digital evidence can be easily altered, deleted, or transferred if not secured promptly. The collection of digital evidence requires specialized technical knowledge and adherence to proper forensic procedures to maintain admissibility in legal proceedings. The intangible nature of such evidence also increases the risk of tampering and poses challenges in establishing authenticity before the judicial systems.

In cyber jurisprudence, proving an offence requires the presence of both actus reus (the wrongful act) and mens rea (the guilty intention). While identifying the act in cybercrime cases may be relatively straightforward, establishing the intention behind such acts is far more complicated. In offences involving computers or automated systems, intent becomes the deciding factor that separates a deliberate crime from an accidental or negligent mistake[12]. For example, unauthorized access to a system may appear harmless unless it can be shown that the access was made with a malicious purpose. Failure to prove such intent can weaken the prosecution's case, as the defense may argue that the conduct was unintentional. The task of

[10] Amos Kipngetich, *A review of online scams and financial frauds in the digital age*, 22(01) GSC Advanced Research and Reviews 305, 302-329 (2025).
[11] *Cyber-Enabled Financial Crime: Intersection of Fraud, AML, and Incident Response*, CANADIAN FINANCIAL CRIME ACADEMY (Feb. 16, 2026, 4:01 PM), https://www.canadianfinancialcrimeacademy.ca/financial-crime-articles/cyber-enabled-financial-crime-intersection-of-fraud-aml-and-incident-response.
[12] *Establishing Mens Rea in Federal Computer Crime Cases*, LEPPARD LAW (Feb. 16, 2026, 6:00 PM), https://federal-criminal.com/computer-crimes/establishing-mens-rea-in-federal-computer-crime-cases/.

proving intention becomes more difficult due to the technical nature of digital evidence and the anonymity provided by cyberspace. Cyber offenders often conceal their identity through tools such as proxy servers or encrypted networks, making it challenging to link a particular act to a specific individual. As a result, prosecutors frequently depend on forensic analysis and expert testimony to demonstrate intention.

The computer-related crimes are held in such a manner that the actual offender rarely interacts with the victim or the targeted system directly. Instead, the offence is carried out through a chain of technological intermediaries such as spoofed IP addresses, VPN networks, botnets, remote servers, encrypted applications, and compromised user accounts. Each of these layers creates a degree of separation between the offender and the criminal act. For instance, when an unauthorised transaction is made through a compromised banking account, the digital trail may only reveal the device or IP address used at the time of access. However, that device may itself have been hacked, remotely controlled, or accessed through another intermediary network. This makes it difficult to determine whether the accused actually intended to commit the offence or whether their system was unknowingly used as a conduit. In some cases, where multiple individuals have access to the same digital infrastructure, such as shared networks or institutional systems, identifying who initiated the act becomes problematic, and proving that the accused possessed the required guilty intention becomes even more challenging. The use of artificial intelligence-based tools adds another layer of complexity, as actions performed by this system may not directly reflect the mental state of the person who deployed them. Therefore, technological layering not only obscures identity but also disrupts the logical connection between the act and the intention behind it, making the establishment of mens rea in cybercrime cases a legally and technically demanding exercise.

III. Current Legal Responses to Phishing Fraud

A) Legal Protection And Enforcement For Victims Of Cyber Crime

Courts in different parts of the country are finding it difficult to decide how financial losses caused by phishing attacks should be covered under the legal framework[13]. With the rapid increase in online transactions, digital communication, and use of internet-based services,

[13] J. Robert MacAneney et al., *2 Circuit Court Rulings Rock Phishing Loss Coverage Field*, LAW 360 (Feb. 21, 2026, 1:58 PM), https://www.law360.com/articles/1067338/2-circuit-court-rulings-rockphishing-loss-coverage-field.

cybercrimes such as phishing, identity theft, online financial fraud, hacking, cyberstalking, and data breaches have become very common. Section 43, Section 66 and Section 72 of Information Technology Act, 2000, deal with offences related to unauthorized access and digital system interference. These provisions involve situations where an individual unlawfully enters, interferes with, or misuses a computer system or digital network without permission. In most phishing and vishing cases, the offence does not begin with cheating; it begins with gaining access to digital credentials, databases, or communication channels through deceptive means. Section 43 addresses acts such as accessing a computer system without authorization, extracting data, introducing malware, or disrupting services. Although it is civil in nature, it becomes relevant in phishing-related financial fraud where login credentials are accessed through fake links and later used to siphon funds. The financial loss suffered by the victim comes from this initial unauthorized entry into their digital account or system. Section 66 criminalizes phishing acts when done dishonestly or fraudulently. For instance, when an attacker installs malicious software through a phishing email attachment or gains unauthorized access to an online banking interface to initiate fraudulent transactions, the offence moves from a compensatory wrong to a punishable criminal act. Section 72 becomes applicable in cases where personal or financial data obtained through authorized system access is misused or disclosed without consent. This assumes importance in vishing scams where insiders, service providers, or telecom agents leak customer information, which is then used by fraudsters to impersonate bank officials and extract OTPs or card details[14]. In this context, these provisions address the technical breach phase which is the stage where digital systems or confidential information are accessed or manipulated before the actual financial cheating takes place.

On the other hand, Section 66C and Section 66D deal with Offences Relating to Identity Misuse and Online Financial Deception. This category directly concerns impersonation-based financial fraud, which lies at the core of phishing and vishing attacks. Section 66C deals with identity theft involving the fraudulent use of another person's password, electronic signature, banking credentials, or any unique identifying information. In phishing scams, victims are tricked into entering their login details on cloned websites, which are later used by offenders to carry out unauthorized transactions. Similarly, in vishing attacks, victims may be persuaded over a phone call to disclose OTPs or card details, enabling fraudsters to assume their digital identity. Section

[14] Sakshat Karkare, *Vishing Attack Explained: How cybercriminals use your voice to steal data*, QUICK HEAL (Feb. 22, 2026, 10:35 AM), https://www.quickheal.co.in/knowledge-centre/vishing-attack-explained-voice-phishing-scam/#:~:text=What%20is%20Vishing%20Attack?,cloud%20data%20safe%20from%20hackers?.

66D addresses cheating by personation using computer resources. This provision becomes particularly relevant in phishing emails that mimic official communication from banks or government agencies, fake job portals seeking registration fees, or voice calls pretending to be from financial institutions. The offender creates a false digital persona to induce trust and manipulate the victim into transferring money or sharing confidential information. Therefore, these provisions govern the deception and financial exploitation phase of cyber fraud. While Sections 43 and 66 address unlawful entry into digital systems, Sections 66C and 66D address the misuse of stolen identity and impersonation tactics that ultimately lead to financial loss.

Apart from punishing offenders, there are clear enforcement mechanisms for recovery of money lost due to cyber fraud[15]. If a person becomes a victim of phishing or UPI fraud (for example, money being transferred after clicking a fake payment link), the first legal step is to immediately report the incident either on the National Cyber Crime Reporting Portal[16] or by calling the 1930 Cyber Financial Fraud Helpline. Once the complaint is registered, the information is automatically forwarded to the concerned bank through the Citizen Financial Cyber Fraud Reporting and Management System[17] (CFCFRMS). This enables the bank to place a debit freeze on the fraudster's account or wallet before the money is withdrawn or layered into multiple accounts. For example, if ₹25,000 is fraudulently transferred through a phishing link and the victim reports it within a few hours, the receiving bank can temporarily block the beneficiary account under RBI-mandated fraud response protocols.

The Reserve Bank of India has issued binding guidelines on "Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions"[18] (2017), which state that if the victim reports the fraud within three working days, the customer shall have zero liability, meaning the bank must refund the entire amount after due verification. If reported between four to seven days, the customer's liability is limited to a fixed amount (for example ₹5,000 or ₹10,000 depending on the type of account). In practice, once the complaint is lodged, the bank initiates a chargeback or lien marking process while the State Cyber Crime Cell traces

[15] Eddy Rifai and H.S. Tisnanta, *Role of Law Enforcement to prevent Cyber laundering and Asset Recovery from Overseas*, 16(1) Int'l J. Cyber Criminology 110, 112 (2022).
[16] NATIONAL CYBER CRIME REPORTING PORTAL, https://cybercrime.gov.in/ (last visited Feb. 21, 11:02 PM).
[17] CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM, https://en.vikaspedia.in/viewcontent/e-governance/citizen-services/citizen-financial-cyber-fraud-reporting-and-management-system (last visited Feb. 21, 11:05 PM).
[18] CUSTOMER PROTECTION – LIMITING LIABILITY OF CUSTOMERS IN UNAUTHORIZED ELECTRONIC BANKING TRANSACTIONS, https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336 (last visited Feb. 21, 11:10 PM).

the digital trail using transaction IDs, IP logs, SIM details, and mule accounts. Based on this, the investigating officer can request account statements under Section 94 of BNSS and initiate prosecution under Sections 66C/66D of the IT Act and cheating provisions of BNS. This system ensures that victims are not only able to initiate criminal action but also have a legally recognized pathway for actual recovery of the defrauded amount through institutional coordination between banks, payment gateways, and cyber police units.

Lastly, CERT-In has issued directions that make it compulsory for organizations to report cyber security incidents such as phishing attacks, data breaches, unauthorized access, identity theft, and leakage of confidential information within a fixed time period[19]. This becomes relevant to identity-based fraud because in many cases victims are not even aware that their personal data has been compromised. Early reporting helps in tracing how stolen information is later used for impersonation, online cheating, or financial fraud. The guidelines also require companies and service providers to maintain system logs for a specified duration so that investigating agencies can track digital footprints in cases involving offences like identity theft or cheating by personation through computer resources.

There is considerable overlap between the provisions of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 when dealing with such cyber-enabled crimes[20]. While the Information Technology Act addresses unauthorized access, identity theft and cheating through computer resources, the Bharatiya Nyaya Sanhita contains general penal provisions relating to cheating, impersonation and breach of trust. However, a major legal gap exists in the absence of explicit statutory recognition of phishing and vishing as separate offences under either of these laws. At present, these fraudulent practices are prosecuted by fitting them into broadly worded provisions relating to cheating, identity theft or unauthorized access. This approach fails to capture the specific nature and evolving techniques used in social engineering attacks. As a result, the legal framework remains reactive rather than preventive. The lack of precise legal classification also creates difficulties in investigation, data collection and policy formulation, as phishing and vishing are treated merely as variants of cheating rather than as technologically distinct forms of cybercrime.

[19] INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Feb. 21, 11:15 PM).
[20] Megha Rodrigues, *Offences Against Cybercrime under the Bharatiya Nyaya Sanhita, 2023 (BNS)*, YOUR LAW ARTICLE (Feb. 21, 2026, 11:20 PM), https://www.yourlawarticle.com/post/offences-against-cybercrime-under-the-bharatiya-nyaya-sanhita-2023-bns.

B) Right to Compensation in Cases of Institutional Negligence

In phishing fraud cases, the financial loss is not always caused solely due to the carelessness of the victim. In many situations, the fraud succeeds because of weak security systems maintained by banks, payment gateways, or digital platforms. Indian cyber law recognizes this possibility and gives victims the right to claim compensation where such institutional negligence has contributed to the loss. Under Section 43 of the Information Technology Act, 2000, if a company or intermediary fails to implement reasonable security practices and this failure results in unauthorized access to a user's account or financial data, the affected individual can seek monetary compensation.

For example, if a phishing transaction takes place even after the victim had enabled transaction alerts, spending limits, or two-factor authentication, and the platform still allowed the transfer without triggering any red flag or fraud detection mechanism, this may indicate a failure on the part of the service provider. Similarly, where a bank fails to block a transaction despite prior reporting by the customer, delays freezing the beneficiary account, or allows repeated suspicious withdrawals within a short time frame, such omissions may amount to deficiency in service. In such cases, the victim is legally entitled to approach the Adjudicating Officer appointed under the IT Act or file a complaint before the Banking Ombudsman to recover the financial loss. This shifts part of the legal responsibility onto the institution and ensures that victims are not unfairly burdened for systemic failures in cybersecurity infrastructure.

C) Right to Protection of Personal and Financial Data During Investigation

Victims of phishing fraud also have the right to confidentiality and protection of their personal information throughout the investigation process. When a complaint is filed, it often includes sensitive data such as bank account numbers, debit or credit card details, Aadhaar information, login credentials, and transaction history. Such information, if not handled securely, may expose the victim to further financial harm or identity theft[21]. To prevent this, cybercrime complaints are processed by specialized cybercrime units like NCFL, that follow data protection protocols during investigation[22]. The victim's personal and financial details are

[21] Justice K.S. Puttaswamy (Retd) v. Union of India, 2019 (1) SCC 1.
[22] Khushhal Kaushik, *India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations*, OBSERVER RESEARCH FOUNDATION (Feb. 22, 2026, 12:19 PM), https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations.

treated as confidential evidence and are shared only with authorized stakeholders such as banks, payment service providers, or investigative agencies strictly for the purpose of tracing the fraudulent transaction. This reduces the risk of secondary misuse of the victim's identity or financial credentials during the pendency of proceedings.

For instance, where a phishing victim has shared OTP or card details on a fake website, there exists a possibility that the stolen data may be reused for future fraudulent transactions. By ensuring restricted access to complaint records and digital evidence, investigating authorities attempt to contain further exposure and safeguard the victim's identity. These procedural safeguards are crucial because phishing fraud does not end with a single transaction; stolen credentials may circulate on the dark web and be exploited repeatedly if not promptly secured. In effect, these rights ensure that victims are not only able to initiate criminal proceedings against offenders but are also protected from continued vulnerability arising out of compromised personal data while the investigation and recovery process is underway.

IV. Emerging Challenges in Cyber Jurisprudence

A) Overdependence on Technology and Role of Artificial Intelligence

Phishing and vishing cannot be solved by using technology or laws alone. It is mainly about managing complex online systems where people often misuse trust for their own benefit[23]. Phishing continues to remain a major cyber security threat despite the availability of multiple mitigation strategies. A key gap identified in existing anti-phishing frameworks is that most of them are heavily technology-driven, with little emphasis on the role played by human users in preventing such attacks[24]. While tools such as spam filters, machine learning-based detection systems, and multi-factor authentication have been developed, their effectiveness is often undermined by user behavior. Individuals tend to act impulsively in situations involving urgency, fear, greed, or curiosity, making them more vulnerable to social engineering tactics used in phishing attacks. Increased digitalization has further expanded the number of access points and devices requiring protection, thereby heightening the risk of exposure. Martin Roesler points out that cybercriminals are usually quick to start using new technologies, and artificial intelligence is just another tool that they have adopted early to improve their

[23] Joseph Savirimuthu, *Identity Theft and the Gullible Computer User: What Sun Tzu in The Art of War Might Teach*, 3(2) J. Int'l Com. L. & Tech. 120, 124 (2008), https://media.neliti.com/media/publications/28767-EN-identity-theft-and-the-gullible-computer-user-what-sun-tzu-in-the-art-of-war-mig.pdf.
[24] 132 BILAL NAQVI ET AL., COMPUTERS & SECURITY 14 (Elsevier, 2023).

methods[25].

B) New Types of Phishing Attacks Not Properly Covered by Existing Systems

At present, most institutional cyber security mechanisms, like Multi-Factor Authentication (MFA)[26], Data Encryption Standard (DES)[27], etc., are designed primarily to detect email-based phishing attempts such as suspicious links, unknown attachments, or spoofed sender addresses. However, it has been observed that fraudsters are increasingly shifting to other forms of phishing attacks which are not effectively monitored by traditional detection tools[28]. For instance, in cases of vishing, individuals receive phone calls from persons impersonating bank officials, telecom authorities, or government representatives and are persuaded to disclose OTPs on the pretext of KYC verification or account reactivation[29]. Similarly, in smishing attacks, fraudulent SMS messages containing shortened URLs are sent to users claiming pending courier deliveries, electricity bill payments, or income tax refunds, which upon being clicked redirect the user to cloned websites resembling legitimate portals such as banking interfaces or UPI platforms[30]. The above-mentioned scenarios show a growing mismatch between the design of institutional cybersecurity tools and the evolving nature of phishing attacks.

Phishing is no longer just a technical or financial fraud issue; it has now created serious legal complications that existing cyber laws are struggling to address. One of the primary challenges in cyber jurisprudence is the difficulty in fixing legal liability when fraud occurs due to user action. In many phishing cases, the victim voluntarily shares OTPs, passwords or banking credentials after being manipulated through social engineering tactics. From a legal standpoint, this creates ambiguity as to whether the loss occurred due to system failure on the part of the bank or due to negligence on the part of the customer. Financial institutions often rely on this

[25] Ansari Zartab Jabeen, *Camouflage of AI in Cyber Crimes Vis-a Vis legal issues and Challenges*, WOXSEN UNIVERSITY (Feb. 21, 2026, 10:43 AM), https://woxsen.edu.in/woxsen-law-review/wlr-papers/camouflage-of-AI-in-cyber-crimes-vis-a-vis-legal-issues-and-challenges/.
[26] JOEY HIRAO, SAP SECURITY CONFIGURATION AND DEVELOPMENT 29-113 (Syngress, 2009).
[27] JOHN F. BUFORD ET AL., P2P NETWORKING AND APPLICATIONS 319-340 (Morgan Kaufmann, 2009).
[28] *Id.* at 16.
[29] The Hindu Bureau, *Hyderabad police caution citizens against rising OTP frauds*, THE HINDU (Feb. 03, 2026, 7:27 PM), https://www.thehindu.com/news/cities/Hyderabad/hyderabad-police-caution-citizens-against-rising-otp-frauds/article70587420.ece.
[30] CYBER CRIME WING, https://cybercrimewing.wb.gov.in/FakeSMSsrelatedtounpaidElectricityBilltodupecitizens (last visited Feb. 19, 2026).

distinction to deny liability by arguing that the transaction was authorized by the account holder, even though such authorization was obtained through deception[31]. This raises important jurisprudential questions regarding the nature of "consent" in digital transactions and whether consent obtained through fraudulent inducement can still be treated as valid consent in cyberspace[32].

V. Need for Legal Reforms in India

A) Enactment of a Separate Anti-Phishing Law

At present, phishing offences in India are dealt with under general provisions relating to cheating, impersonation, identity theft, or unauthorized access under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. However, phishing is not an ordinary cheating offence. It is a technologically enabled form of deception which involves fake websites, cloned emails, malicious links, and social engineering techniques to trick individuals into disclosing confidential information such as OTPs, passwords, or banking details. Since there is no specific legislation that directly defines and criminalizes phishing as a distinct cyber offence, law enforcement agencies are forced to fit such cases into existing legal provisions that were never designed to address online financial fraud. This creates legal ambiguity and delays in investigation and prosecution.

Therefore, there is a pressing need to introduce a dedicated Anti-Phishing Act in India, similar to legislative measures adopted in other technologically advanced countries. Such a law can clearly define phishing, vishing, smishing, and related cyber-deception practices, lay down investigation procedures, and prescribe institutional responsibilities for banks and digital intermediaries. A specialized legal framework will make it easier for cybercrime units to register offences without confusion and ensure uniform application of law across different states.

B) Recognition of Phishing as a Specific Criminal Offence

In Canada, phishing is a crime and the penalty is 14 years imprisonment[33]. In the same way,

[31] Jo Braithwaite, *Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?* 10 J. Fin. Reg. 179, 174-193 (2024).
[32] Gaurav Thote, *Unravelling "Consent" under the Digital Personal Data Protection Act, 2023 — A Barrier to Data Principal Rights*, SCC ONLINE (Feb. 19, 2026, 11:57 PM), https://www.scconline.com/blog/post/2024/11/13/unravelling-consent-under-the-digital-personal-data-protection-act-2023-a-barrier-to-data-principal-rights/.
[33] CANADIAN ANTI-FRAUD CENTRE, https://antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-

phishing should be treated as an independent criminal offence in the same way as robbery, fraud, or criminal breach of trust. At present, phishing is indirectly prosecuted by applying general provisions relating to cheating or identity theft. However, this approach ignores the complex digital infrastructure involved in phishing attacks. This form of deception involves both technological manipulation and behavioral exploitation, which distinguishes it from traditional fraud. By recognizing phishing as a standalone offence, the law can specifically address acts such as creation of spoofed domains, transmission of deceptive communication links, or impersonation through digital platforms. This will also help courts in accurately categorizing the offence rather than stretching conventional definitions of cheating to cover cyber-enabled fraud.

Additionally, the present penal provisions applicable to cyber fraud do not adequately reflect the seriousness of phishing attacks. In many cases, phishing scams result in substantial financial losses affecting multiple victims simultaneously. Fraudsters often target elderly individuals, first-time digital banking users, or persons with limited technological awareness. The punishment prescribed under existing laws may not act as a sufficient deterrent, especially when cybercriminals operate through organized networks[34]. Stricter penalties, including higher fines and longer terms of imprisonment, may serve as an effective deterrent against such offences. Enhanced punishment may also be justified where the offence involves repeat offenders, large-scale financial fraud, or misuse of sensitive personal data. Introducing graded punishment based on the extent of financial damage or number of victims affected can ensure proportionality while strengthening the preventive role of criminal law.

C) Use of Artificial Intelligence for Early Detection of Phishing Scams

Legal reform must also be accompanied by technological intervention in order to effectively curb phishing attacks. Artificial intelligence-based detection systems can be integrated into banking networks, email servers, and digital payment platforms to identify suspicious communication patterns or unauthorized login attempts[35]. AI tools can analyze transaction

service-hameconnage-eng.htm (last visited Feb. 22, 2026).

[34] Nadia Khadam et al., *How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan*, 9(12) Heliyon 1, 6 (2023).

[35] Sheed Iseal and Michael Halli, *AI-Powered Fraud Detection in Digital Payment Systems: Leveraging Machine Learning for Real-Time Risk Assessment*, Research Gate (last visited Feb. 22, 2026, 11:55 PM), https://www.researchgate.net/publication/388675296_AI-Powered_Fraud_Detection_in_Digital_Payment_Systems_Leveraging_Machine_Learning_for_Real-Time_Risk_Assessment.

behavior in real time and flag unusual transfers, thereby enabling institutions to block fraudulent transactions before completion. For instance, if a sudden transaction is initiated from an unfamiliar device or geographic location immediately after a user clicks on a suspicious link, an AI-enabled fraud detection mechanism can automatically freeze the transaction and alert the account holder. Such automated systems can significantly reduce the time gap between occurrence of fraud and reporting, which is crucial for financial recovery. Incorporating AI-driven monitoring within regulatory frameworks will therefore enhance both preventive and investigative capabilities in dealing with phishing offences[36]. In this manner, a combination of legislative clarity and technological support can strengthen the existing cyber law regime and provide more effective protection to victims of phishing fraud in India.

VI. Conclusion

Phishing has become one of the most common and dangerous forms of cybercrime in today's digital world. With the increasing use of online banking, digital payments, and internet-based services, individuals are constantly exposed to the risk of fraud through fake emails, messages, and websites. These scams do not involve force or physical theft, but instead rely on deception and misuse of technology to gain access to sensitive personal and financial information. As a result, victims often suffer serious financial loss within a very short span of time.

Although India has legal provisions under existing cyber laws to deal with such offences, the absence of a specific legal framework exclusively addressing phishing creates practical difficulties in investigation, prosecution, and enforcement. Many cases are still dealt with under general provisions relating to cheating or impersonation, which may not fully capture the nature and complexity of phishing attacks. This highlights the urgent need for legal reform in order to recognize phishing as a distinct cyber offence and ensure that appropriate punishment and preventive mechanisms are put in place. Further, strengthening the role of technological tools such as artificial intelligence in fraud detection can assist both financial institutions and investigating agencies in responding to phishing incidents more effectively. Timely reporting, improved legal clarity, stricter penalties, and advanced monitoring systems can together reduce the success rate of such scams and enhance public confidence in digital transactions.

In conclusion, addressing phishing fraud requires a balanced approach involving legal

[36] Luis A. Garcia-Segura, *The role of artificial intelligence in preventing corporate crime*, 5 J. Econ. Criminology 1, 2 (2024).

development, institutional responsibility, and user awareness. By adapting the legal system to meet the challenges posed by evolving cyber threats, it is possible to provide better protection to victims and ensure accountability in the digital environment.