INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

Phishing and online identity theft: An analysis of legal remedies and challenges in India

Babitha. W.K

School of Excellence in Law, Tamilnadu Dr. Ambedkar Law University

www.ijlra.com

ABOUT THE JOURNAL

International Journal for Legal Research and Analysis (IJLRA)

ISSN: 2582-6433

IJLRA provides a platform for scholarly writing and discussion on law, legal research and interdisciplinary questions. Research articles explore legal principles, institutions, policy and contemporary developments.

Journal website: www.ijlra.com

PUBLICATION INFORMATION

International Journal for Legal Research and Analysis

ISSN: 2582-6433

Editorial note

The views and arguments expressed in this article are those of its author(s). Readers should consult the original legal authorities and sources cited in the manuscript.

Copyright and permissions are subject to the applicable publication agreement.

ARTICLE DETAILS

Phishing and online identity theft: An analysis of legal remedies and challenges in India

Author: Babitha. W.K

Institution: School of Excellence in Law, Tamilnadu Dr. Ambedkar Law University

Journal: International Journal for Legal Research and Analysis

ISSN: 2582-6433

Phishing and online identity theft: An analysis of legal remedies and challenges in India

Babitha. W.K

School of Excellence in Law, Tamilnadu Dr. Ambedkar Law University

Abstract

The rapid development of internet technology and digital financial services has made online transactions an essential part of everyday life. Banking, shopping, communication and several other activities are now carried out through digital platforms. Although these developments have made life easier, they have also created opportunities for cybercriminals to exploit individuals through fraudulent online activities. Phishing and online identity theft are two such cybercrimes that have become increasingly concerning in India. Phishing generally involves the use of fraudulent emails, messages, websites or telephone communications to deceive individuals into revealing confidential information such as passwords, banking details, One-Time Passwords (OTPs) and other personal data. Online identity theft occurs when such information is fraudulently obtained and used to impersonate another person, access accounts or carry out unauthorised financial transactions.

The present study examines the nature and methods of phishing and online identity theft, with particular reference to the legal framework available in India. It analyses the relevant provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other applicable laws and regulatory measures. It also examines the role of the Reserve Bank of India,

CERT-In, cybercrime reporting mechanisms and law enforcement authorities in preventing and addressing these offences. Further, the paper identifies practical challenges relating to investigation, jurisdiction, electronic evidence, recovery of financial losses and victim protection.

The study argues that although India has established a legal framework to address cyber fraud, effective enforcement, public awareness, institutional coordination and timely remedies remain essential to ensure meaningful protection against these offences.

Keywords: Phishing, Online Identity Theft, Cybercrime, Information Technology Act, 2000,

Digital Fraud, Data Protection, Cybersecurity, India.

Chapter I – Introduction

1.1 Introduction

The growth of information and communication technology has brought significant changes to the way individuals communicate, conduct business and manage their financial activities. The increasing use of smartphones, internet banking, digital payment applications and social media platforms has made digital services easily accessible to people across the country. In India, initiatives promoting digital transactions have further encouraged individuals to depend on online platforms for their everyday requirements.

However, the increasing dependence on digital technology has also resulted in the emergence of different forms of cybercrime. Unlike traditional offences, cybercrimes are often committed through digital networks, allowing offenders to target individuals without having direct physical contact with them. Among these offences, phishing and online identity theft have become serious concerns because they directly affect an individual's financial security, privacy and personal identity.

Phishing is a fraudulent technique through which cybercriminals attempt to obtain confidential information by pretending to be genuine individuals, organisations or institutions. For example, a person may receive a message appearing to come from a bank stating that their account will be blocked unless they immediately update their KYC details through a given link. When the individual clicks the link and enters their banking credentials, the information is collected by the fraudster and may subsequently be used to access the victim's account.

Online identity theft is closely connected with phishing. Once personal information, passwords, banking credentials or other identification details are obtained, criminals may use them to impersonate the victim. Such information may be misused to conduct financial transactions, create fraudulent accounts, obtain loans, access social media profiles or commit further offences in the victim's name.

What makes these offences particularly dangerous is that the victim may not immediately realise that their identity or personal information has been compromised. Even after discovering the fraud, recovering the lost money and identifying the actual offender can be difficult. In many situations, the criminals operate through multiple accounts, fake identities, temporary mobile numbers and intermediaries, making investigation more complicated.

In India, the Information Technology Act, 2000 provides specific provisions dealing with identity theft and cheating by personation through computer resources. In addition, the Bharatiya

Nyaya Sanhita, 2023 contains provisions relating to cheating and cheating by personation.

Regulatory authorities such as the Reserve Bank of India and CERT-In also play an important role in addressing different aspects of cyber fraud.

Therefore, this research examines whether the existing legal framework provides sufficient protection against phishing and online identity theft and whether the available legal remedies are practically effective in protecting victims.

1.2 Meaning of Phishing

Phishing is a form of cyber fraud in which an offender attempts to deceive an individual into disclosing sensitive information by pretending to represent a trustworthy person or organisation.

The communication may take place through emails, SMS messages, telephone calls, social media accounts or fraudulent websites.

The term is commonly associated with the practice of using deceptive communications to obtain passwords, banking information, OTPs and other confidential details. The information collected may subsequently be used for unauthorised access, financial fraud or identity theft.

For example, a person may receive an SMS claiming to be from a bank, requesting them to update their KYC information immediately. The message contains a link that directs the

individual to a website resembling the bank's official website. When the individual enters their account details, the information is captured by the fraudster.

The important element in phishing is deception. The offender creates a false sense of trust or urgency so that the victim voluntarily provides information that would otherwise remain confidential.

1.3 Meaning of Online Identity Theft

Online identity theft refers to the fraudulent acquisition and use of another person's identifying information without their consent or lawful authority.

Such information may include:

- Name, address and date of birth.
- Bank account and payment details.
- Passwords and login credentials.
- Aadhaar-related identification information.
- PAN details and other identification documents.
- Email and social media account credentials.
- Digital signatures and other electronic identification features.

Identity theft does not necessarily involve financial loss in every situation. A person may also suffer reputational damage, loss of privacy, harassment or legal difficulties because another individual has used their identity for unlawful activities.

For instance, a fraudster may use another person's identity documents to open an account or create a fake social media profile. The actual individual may subsequently face difficulties when the account is used for fraudulent transactions.

1.4 Relationship Between Phishing and Online Identity Theft

Phishing and online identity theft are separate but closely connected cyber offences.

Phishing is generally the method through which confidential information is obtained, whereas identity theft involves the unauthorised use of another person's identifying information.

The relationship can be understood through the following example:

1. A fraudster sends a fake banking message to an individual.
2. The individual clicks the fraudulent link.
3. The individual enters their username, password and OTP.
4. The fraudster obtains access to the victim's banking account.
5. The information is used to conduct unauthorised transactions.
6. The victim suffers financial loss and possible misuse of personal identity.

Thus, phishing may act as the starting point for identity theft and other forms of cyber fraud.

However, identity theft can also occur through data breaches, malware, social engineering and other methods without phishing.

1.5 Statement of the Research Problem

The increasing use of digital platforms has created new opportunities for cybercriminals to obtain and misuse personal information. Although India has enacted legislation to address cyber offences, phishing and online identity theft continue to create difficulties for individuals and investigating authorities.

The primary problem is not merely the absence of legal provisions but also the difficulty in implementing them effectively. Victims may not know where to report an incident, how to preserve digital evidence or which authority is responsible for providing assistance. Further, cybercriminals frequently operate through multiple accounts, anonymous identities and different geographical locations, making it difficult to identify the actual offenders.

Another major concern is the recovery of money lost through fraudulent transactions. Even when a complaint is registered, the victim may face delays in tracing the transferred funds or obtaining appropriate relief.

Therefore, the research problem concerns the adequacy and effectiveness of existing Indian legal remedies in addressing phishing and online identity theft, particularly in relation to investigation, punishment, financial recovery and protection of victims.

1.6 Objectives of the Study

The objectives of this research are:

1. To examine the meaning, nature and development of phishing and online identity theft.

2. To identify the different methods used by cybercriminals to commit these offences.

3. To analyse the legal provisions relating to phishing and identity theft under Indian law.

4. To examine the legal remedies available to victims of phishing and online identity theft.

5. To study the role of regulatory authorities and law enforcement agencies in preventing cyber fraud.

6. To identify the practical and legal challenges involved in investigating these offences.

7. To suggest suitable legal and institutional measures for improving cybersecurity and victim protection.

1.7 Research Questions

1. What are phishing and online identity theft, and how do they affect individuals in India?

2. Whether the existing provisions of the Information Technology Act, 2000 adequately address phishing and online identity theft?

3. What legal remedies are available to victims who suffer financial loss or misuse of personal information?

4. What difficulties are faced by law enforcement authorities in investigating and prosecuting these offences?

5. What measures can be introduced to strengthen the existing legal framework and protect individuals against cyber fraud?

1.8 Hypothesis

The existing legal framework in India provides various remedies to address phishing and online identity theft. However, difficulties relating to cyber investigation, identification of offenders, jurisdiction, electronic evidence and recovery of financial losses affect the effective implementation of these legal remedies.

1.9 Research Methodology

The present research adopts a doctrinal research methodology. It is based on the examination of primary and secondary legal sources, including statutes, judicial decisions, government notifications, regulatory guidelines, books, research articles and reports relating to cybercrime and data protection.

Primary sources include the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita,

2023, the Digital Personal Data Protection Act, 2023, relevant provisions of the Bharatiya

Sakshya Adhiniyam, 2023 and Reserve Bank of India guidelines.

Secondary sources include academic publications, research papers, legal commentaries and materials published by government authorities and cybersecurity institutions.

The study is primarily analytical and focuses on examining the adequacy of existing legal remedies and the practical difficulties involved in their implementation.

Chapter II – Nature and Methods of Phishing and Online Identity Theft

2.1 Evolution of Phishing and Online Identity Theft

The development of phishing is closely associated with the growth of internet communication and online financial services. In the earlier stages of internet usage, cyber fraud was commonly carried out through deceptive emails and fake online messages. Offenders attempted to obtain usernames and passwords by pretending to be representatives of genuine organisations.

With the development of online banking, e-commerce and digital payment systems, these activities gradually became more sophisticated. Fraudsters began using websites that closely resembled the original websites of banks and other financial institutions. The introduction of smartphones and social media platforms further expanded the methods through which individuals could be targeted.

In recent years, phishing has moved beyond traditional email fraud. Criminals now use SMS messages, instant messaging applications, fake customer-care numbers, QR codes, social media advertisements and fraudulent mobile applications. Some offenders also use artificial intelligence to create convincing messages and impersonate genuine individuals.

Similarly, online identity theft has developed from the unauthorised use of basic login credentials into more complex forms of impersonation involving personal documents, financial information and digital identities.

This development shows that phishing and identity theft are no longer limited to technical attacks against computer systems. They increasingly involve psychological manipulation, misuse of personal information and exploitation of people's trust in digital services.

2.2 Different Types of Phishing

Phishing can be carried out through several methods depending on the communication platform used by the offender.

1. Email Phishing

Email phishing involves sending fraudulent emails that appear to originate from banks, government departments, financial institutions or other trusted organisations. The emails generally contain links or attachments intended to obtain confidential information or install malicious software.

2. Spear Phishing

Spear phishing is a targeted form of phishing in which the offender collects information about a particular individual or organisation before sending a fraudulent communication. Unlike general phishing messages, these communications may contain the victim's name, workplace or other personal details, making them appear more genuine.

3. Smishing

Smishing refers to phishing carried out through SMS messages. Victims may receive messages claiming that their bank account will be suspended, their parcel cannot be delivered or their KYC verification is incomplete. Such messages usually contain fraudulent links or telephone numbers.

4. Vishing

Vishing involves the use of telephone calls to deceive individuals into revealing confidential information. Fraudsters may pretend to be bank officials, police officers, customer-care representatives or government employees. They may create fear or urgency to persuade victims to disclose OTPs, passwords or banking details.

5. Clone Phishing

In clone phishing, an offender creates a copy of a previously received genuine email or message and replaces its original attachment or link with a malicious one. Since the communication resembles an earlier legitimate message, the victim may not suspect fraudulent activity.

6. Pharming

Pharming involves redirecting users from a genuine website to a fraudulent website without their knowledge. This may occur through manipulation of DNS settings or other technical methods.

Unlike ordinary phishing, the victim may enter the correct website address and still be redirected to a fake website.

7. QR Code Phishing (Quishing)

QR code phishing involves using fraudulent QR codes to direct individuals to malicious websites or payment interfaces. In some cases, victims are deceived into scanning a code under

the impression that they will receive money, whereas the process may expose them to financial fraud.

8. Social Media Phishing

Social media phishing involves creating fake profiles or impersonating genuine accounts to obtain personal information. Offenders may send fraudulent investment offers, prize announcements, job opportunities or emergency requests for money.

2.3 Methods of Online Identity Theft

Online identity theft may take place through different methods, including the following:

1. Credential Theft: Criminals obtain passwords and login details through fake websites, malicious applications or fraudulent communications.

2. Account Takeover: After obtaining login credentials, offenders gain unauthorised access to the victim's email, banking or social media accounts and use them for unlawful purposes.

3. SIM Swapping: Criminals fraudulently obtain control over a victim's mobile number by manipulating mobile service procedures. This may allow them to receive OTPs and other verification messages.

4. Misuse of Personal Documents: Identity documents and personal information may be collected through fraudulent websites or data breaches and subsequently used to impersonate the individual.

5. Synthetic Identity Fraud: Offenders combine genuine personal information with fabricated details to create an identity that does not genuinely belong to one individual.

6. Social Engineering: Criminals manipulate victims into voluntarily revealing confidential information by creating false situations involving financial emergencies, employment opportunities or official verification procedures.

2.4 Impact of Phishing and Online Identity Theft

Phishing and online identity theft affect individuals in several ways.

● Financial loss: Victims may lose money through unauthorised bank transfers, fraudulent card transactions and digital payment applications.

● Violation of privacy: Personal and confidential information may be collected, disclosed or misused without consent.

● Reputational damage: Criminals may use another person's identity to send fraudulent messages, create fake profiles or participate in unlawful activities.

● Mental distress: Victims may experience anxiety, embarrassment and a loss of confidence in digital financial services.

● Legal complications: Individuals may be required to establish that transactions or accounts created in their names were not authorised by them.

● Loss of trust: Repeated cyber fraud incidents may discourage individuals from using online banking and other digital services.

Therefore, the consequences of these offences extend beyond financial loss and affect an individual's privacy, dignity and security.

Chapter III – Legal Framework Governing Phishing and Online Identity Theft in India

India addresses phishing and online identity theft through a combination of cyber laws, general criminal law, data protection legislation and regulatory measures.

3.1 Information Technology Act, 2000

The Information Technology Act, 2000 is the principal legislation dealing with electronic transactions and several forms of cybercrime in India. It was enacted to provide legal recognition to electronic records and digital transactions and to address offences involving computer resources and communication devices.

The Act was subsequently amended in 2008 to introduce additional provisions addressing emerging cyber offences, including identity theft and cheating by personation through computer resources.

The following provisions are particularly relevant to the present research.

Section 43 – Penalty and Compensation for Damage to Computer, Computer System, etc.

Section 43 deals with unauthorised activities involving computer systems and networks. It covers acts such as unauthorised access, downloading or copying information, introducing computer contaminants and damaging computer systems.

This provision may become relevant where a phishing operation involves unauthorised access to computer resources or the copying and extraction of information without permission.

The person responsible may be required to pay compensation to the affected individual.

However, Section 43 is primarily concerned with unauthorised acts involving computer resources. It should not be treated as automatically applicable to every phishing communication.

Section 66 – Computer-Related Offences

Section 66 provides criminal punishment for acts referred to under Section 43 when they are committed dishonestly or fraudulently.

The punishment may extend to imprisonment for three years, or a fine which may extend to five lakh rupees, or both.

For example, if an offender dishonestly accesses another person's computer account or obtains confidential information through unauthorised access, this provision may become applicable depending on the facts of the case.

Section 66C – Punishment for Identity Theft

Directly relevant provision

Section 66C specifically deals with identity theft. It provides punishment for any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of another person.

The punishment may extend to imprisonment for three years and a fine which may extend to one lakh rupees.

This provision is particularly important in cases where offenders misuse another person's passwords, electronic signatures or unique identification features to access accounts or conduct fraudulent activities.

For example, if a person obtains another individual's banking password through phishing and uses it to access the victim's account, Section 66C may be attracted, subject to proof of the statutory ingredients.

Section 66D – Cheating by Personation Using Computer Resources

Section 66D addresses cheating by personation through communication devices or computer resources.

The provision is especially relevant to phishing because cybercriminals frequently pretend to be bank officials, government representatives or other trusted persons to deceive victims.

The punishment under this section may extend to imprisonment for three years and a fine which may extend to one lakh rupees.

For example, when an offender creates a fake customer-care profile and pretends to represent a bank to obtain confidential information from an individual, the conduct may attract Section 66D.

Section 66E – Violation of Privacy

Section 66E deals with the intentional or knowing capture, publication or transmission of images of a person's private area without consent, under circumstances violating privacy.

It may be relevant to certain identity-related cyber offences involving the misuse of private images. However, it is not a general provision covering every form of personal data theft.

Section 72 – Breach of Confidentiality and Privacy

Section 72 deals with the disclosure of information obtained through powers conferred under the

Information Technology Act without the consent of the person concerned or in breach of the conditions prescribed by law.

Its application is limited to the circumstances specified in the provision. It does not automatically cover every private individual's unauthorised disclosure of another person's information.

Section 72A – Disclosure of Information in Breach of Lawful Contract

Section 72A provides punishment where a person, including an intermediary, discloses personal information obtained while providing services under a lawful contract, without the consent of the person concerned or in breach of the lawful contract, with the intention or knowledge of causing wrongful loss or wrongful gain.

This provision may be relevant when personal information collected by service providers is improperly disclosed and subsequently misused.

Section 75 – Act to Apply for Offence or Contravention Committed Outside India

Section 75 extends the application of the Information Technology Act to certain offences and contraventions committed outside India where the conduct involves a computer, computer system or computer network located in India.

This provision is important because phishing operations frequently involve offenders, servers and financial intermediaries located in different countries.

Section 79 – Exemption from Liability of Intermediary in Certain Cases

Section 79 provides conditional protection to intermediaries from liability for third-party information, subject to compliance with statutory requirements and due diligence obligations.

It is relevant when examining the responsibilities of online platforms and intermediaries in relation to unlawful content and misuse of their services. However, intermediary protection is not an unconditional exemption from legal responsibility.

The above provisions demonstrate that the Information Technology Act provides a foundation for addressing different aspects of phishing and identity theft.

India Code+1

3.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code, 1860 with effect from 1 July 2024. It contains provisions that may be applied alongside the Information

Technology Act when phishing and identity theft involve cheating, impersonation and financial fraud.

Section 318 – Cheating

Section 318 defines cheating as deceiving a person and fraudulently or dishonestly inducing them to deliver property, consent to the retention of property or do or omit to do something that causes or is likely to cause harm.

This provision is relevant to phishing because offenders generally deceive victims into transferring money or disclosing information that facilitates financial loss.

Section 318(4) provides punishment of imprisonment which may extend to seven years and also a fine where cheating dishonestly induces the delivery of property or the making, alteration or destruction of a valuable security.

Section 319 – Cheating by Personation

Section 319 specifically deals with cheating by personation.

It applies when a person cheats by pretending to be someone else or knowingly represents themselves or another person as someone different from their actual identity.

This provision is particularly relevant when fraudsters impersonate bank employees, government officers or other individuals to deceive victims.

The punishment may extend to imprisonment for five years, or a fine, or both.

The provisions of Sections 318 and 319 may operate alongside Section 66D of the Information

Technology Act, depending on the nature of the conduct and the ingredients of the offences established.

IndiaCode+2

Important legal distinction: The BNS came into force on 1 July 2024. Offences committed before that date must be considered under the applicable law in force when the offence occurred, subject to the relevant savings provisions. Therefore, older cases may still refer to Sections 415,

416, 419 and 420 of the Indian Penal Code.

3.3 Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, governs the admissibility and proof of evidence in judicial proceedings.

Electronic evidence is particularly important in phishing and identity theft cases because the investigation may depend on:

● Fraudulent emails and SMS messages.

● Screenshots of fraudulent websites.

● Bank transaction records.

● IP addresses and server logs.

● Call recordings and telephone records.

● Social media communications.

● Digital payment transaction details.

Section 63 of the BSA deals with the admissibility of electronic records and prescribes requirements concerning computer outputs and certification.

This provision is important because digital evidence must be properly collected, preserved and produced before a court. Merely submitting a screenshot or downloaded message may not, by itself, establish its authenticity.

In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Supreme Court explained the importance of compliance with Section 65B of the Indian Evidence Act, 1872 for proving secondary electronic evidence under the earlier evidentiary framework. The decision remains important when understanding the principles of authenticity and certification, although the present statutory framework is governed by the BSA.

Sci API+1

3.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted to regulate the processing of digital personal data and recognise the rights of individuals concerning their personal information.

The legislation is relevant to online identity theft because the unauthorised collection, disclosure and misuse of personal data can expose individuals to impersonation and other cyber offences.

Some important aspects of the Act include:

● Section 4: Provides the general framework for processing digital personal data for lawful purposes.

● Section 5: Deals with notice requirements.

● Section 6: Addresses consent and the requirements for valid consent.

● Section 8: Provides for the general obligations of Data Fiduciaries.

● Section 11: Recognises the right of a Data Principal to obtain information about personal data processing.

● Section 12: Provides for correction, completion, updating and erasure of personal data.

● Section 13: Provides for grievance redressal.

● Section 27: Deals with the powers and functions of the Data Protection Board of India.

The Act is relevant where personal information is improperly processed or exposed by entities responsible for handling it.

However, it is important to understand that the DPDP Act is not a criminal punishment statute for phishing. Criminal liability for phishing and identity theft is principally addressed through the

Information Technology Act and applicable criminal law.

Position as on 23 November 2026: The DPDP Act has a phased commencement framework.

The notification dated 13 November 2025 provides for different commencement dates, with several substantive provisions, including Sections 3–17, scheduled to commence eighteen months after publication, i.e. 13 May 2027. Therefore, these provisions should not be incorrectly described as already fully operational.

3.5 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 provides remedies to consumers against deficiencies in services and unfair trade practices.

In certain situations, victims of digital financial fraud may approach consumer dispute redressal mechanisms where the dispute involves a deficiency in a service provided by a bank or other service provider.

However, a consumer complaint is not automatically maintainable merely because a person has suffered phishing fraud. The victim must establish the relevant consumer relationship and the deficiency or other legally recognised ground against the service provider.

3.6 Constitutional Protection of Privacy

The Constitution of India does not expressly mention a separate fundamental right to data protection. However, the Supreme Court has recognised privacy as a fundamental right under

Article 21 and other constitutional freedoms.

In Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, a nine-judge Constitution

Bench unanimously recognised the right to privacy as a constitutionally protected right.

The judgment recognised that privacy is closely connected with dignity, personal autonomy and individual liberty.

This principle is relevant to online identity theft because the misuse of an individual's personal information affects their ability to control how their identity and private information are used.

The judgment also established that restrictions on privacy must satisfy requirements relating to legality, legitimate State purpose, necessity and proportionality.

Chapter IV – Legal Remedies Available to Victims in India

The availability of legal provisions alone is not sufficient unless victims can access them without unnecessary delay. Indian law provides different remedies depending on the nature of the fraud, the financial loss involved and the manner in which personal information has been misused.

4.1 Filing a Complaint through the National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal is an important mechanism established by the

Government of India to enable individuals to report cybercrime incidents.

The portal allows victims to report different forms of cyber offences, including online financial fraud and identity-related offences.

Victims can submit complaints through:

National Cyber Crime Reporting Portal

The portal provides a mechanism for submitting complaints and forwarding them to the appropriate law enforcement authorities for further action.

In cases involving financial fraud, victims should report the incident immediately and provide relevant information such as transaction details, bank account information, mobile numbers, screenshots and other available evidence.

4.2 Reporting Financial Cyber Fraud through Helpline 1930

The national cyber financial fraud helpline, 1930, is an important initiative for reporting financial cybercrime.

A person who discovers an unauthorised financial transaction should immediately contact 1930

and provide the required transaction and identification details.

The objective is to facilitate prompt communication with the concerned financial institutions and support the process of placing holds or preventing further movement of the transferred funds, wherever possible.

However, reporting a transaction does not guarantee that the entire amount will be recovered.

The possibility of recovery depends on factors such as the time taken to report the incident, the movement of funds and the availability of money in the receiving accounts.

4.3 Reporting to the Concerned Bank or Financial Institution

A victim of phishing-related banking fraud should immediately inform the concerned bank or financial institution.

The complaint should contain:

1. Date and time of the fraudulent transaction.

2. Amount involved.

3. Bank account or payment details.

4. Transaction identification number.

5. Details of the fraudulent communication, if available.

6. Copy of the cybercrime complaint or acknowledgement.

The bank should be requested to block compromised banking credentials, secure the account and investigate the unauthorised transaction.

The victim should also preserve the complaint acknowledgement and all communications exchanged with the bank.

4.4 Remedies under RBI Guidelines

The Reserve Bank of India has issued directions concerning customer protection and liability in unauthorised electronic banking transactions.

The RBI's circular dated 6 July 2017, titled Customer Protection – Limiting Liability of

Customers in Unauthorised Electronic Banking Transactions, established a framework for determining customer liability.

The framework distinguishes between different situations:

1. Bank's negligence or deficiency

Where an unauthorised transaction occurs due to contributory fraud, negligence or deficiency on the part of the bank, the customer may have zero liability.

2. Third-party breach

Where the fault lies neither with the bank nor the customer but elsewhere in the system, the customer's liability depends on the time taken to report the transaction.

Under the 2017 framework, reporting within three working days generally attracts zero customer liability. Reporting within four to seven working days attracts limited liability according to the applicable account category and transaction limits. Reporting after seven working days is governed by the bank's board-approved policy.

3. Customer negligence

Where the unauthorised transaction occurs because of the customer's negligence, such as sharing payment credentials, the customer generally bears the loss until the transaction is reported to the bank. Any loss occurring after reporting is generally borne by the bank.

These protections must be understood carefully. Sharing an OTP or password may affect liability, but it does not automatically mean that every claim against the bank must fail. The circumstances, applicable RBI directions and the conduct of the bank must be examined.

The RBI has subsequently consolidated and revised relevant instructions, including through its

2025 Directions and 2026 amendment for commercial banks. Accordingly, the applicable directions should be checked for the relevant bank and transaction date rather than relying exclusively on the original 2017 circular.

4.5 Criminal Remedies

Victims may approach the police or appropriate cybercrime investigation authorities to initiate criminal proceedings against the offenders.

Depending on the facts, the following provisions may be invoked:

Legal provision Nature of offence

IT Act, Section 66 Dishonest or fraudulent computer-related acts under Section 43

IT Act, Section 66C Identity theft

IT Act, Section 66D Cheating by personation using computer resources

BNS, Section 318 Cheating

BNS, Section 319 Cheating by personation

The specific provisions invoked will depend on the evidence and the ingredients of each offence.

4.6 Civil Compensation and Other Remedies

Apart from criminal proceedings, victims may seek compensation where the legal requirements are satisfied.

Section 43 of the IT Act provides for compensation for specified unauthorised acts involving computer resources. Section 46 provides for adjudication of specified contraventions and claims for compensation or penalty under the Act.

Victims may also explore appropriate civil proceedings against persons or entities responsible for legally actionable loss.

Where a bank or financial institution has failed to comply with applicable regulatory obligations, the victim may use the bank's grievance redressal mechanism and, where eligible, approach the

RBI's Complaint Management System under the RBI Integrated Ombudsman Scheme.

The Ombudsman mechanism may provide relief in eligible complaints involving deficiencies in regulated financial services, subject to the applicable scheme and procedural requirements.

Chapter V – Role of Authorities in Preventing Phishing and Online Identity Theft

The prevention of phishing and identity theft cannot be achieved through criminal legislation alone. It requires the combined efforts of government authorities, financial institutions, cybersecurity organisations and law enforcement agencies.

5.1 Indian Computer Emergency Response Team (CERT-In)

Indian Computer Emergency Response Team (CERT-In)

CERT-In operates under the Ministry of Electronics and Information Technology and functions as the national agency for responding to cybersecurity incidents.

Its responsibilities include:

- Collecting and analysing information relating to cybersecurity incidents.
- Issuing alerts and advisories about emerging cyber threats.
- Providing guidance on preventing and responding to cyber incidents.
- Coordinating cybersecurity responses with relevant organisations.
- Supporting the reporting and investigation of cybersecurity incidents.

Under Section 70B of the Information Technology Act, 2000, CERT-In has statutory responsibilities relating to cybersecurity incident response.

The CERT-In Directions dated 28 April 2022 require specified entities, including service providers, intermediaries, data centres, body corporates and government organisations, to report specified cyber incidents within six hours of noticing them or being informed of them.

These directions also prescribe requirements relating to the maintenance of logs and other cybersecurity practices. They are relevant to phishing because timely incident reporting and preservation of technical records may assist in identifying and responding to cyber threats.

Official website: CERT-In

5.2 Reserve Bank of India (RBI)

The Reserve Bank of India plays an important role in protecting customers against fraudulent electronic banking transactions.

Its responsibilities include:

- Issuing directions to banks concerning digital payment security.
- Establishing customer protection standards.
- Requiring banks to maintain appropriate security systems.
- Providing a framework for determining customer liability.
- Regulating grievance redressal mechanisms for banking customers.

The RBI's customer protection directions are particularly important because phishing frequently results in unauthorised financial transactions.

Official website: Reserve Bank of India

5.3 National Cyber Crime Coordination Centre (I4C)

Indian Cyber Crime Coordination Centre (I4C) functions under the Ministry of Home Affairs.

It was established to improve coordination among law enforcement agencies and strengthen the response to cybercrime.

Its major functions include:

- Coordinating cybercrime investigations.
- Supporting cybercrime analysis and intelligence sharing.
- Facilitating cooperation between central and state agencies.
- Supporting cybercrime awareness and capacity-building programmes.

● Providing institutional support for the National Cyber Crime Reporting Portal and related cybercrime response mechanisms.

The I4C is especially important in cases involving multiple bank accounts, mobile numbers and geographical locations.

Official website: Indian Cyber Crime Coordination Centre

5.4 National Payments Corporation of India (NPCI)

National Payments Corporation of India operates and manages important retail payment infrastructure, including the Unified Payments Interface (UPI).

Its role is relevant to phishing because digital payment systems are frequently misused by offenders to transfer money obtained through fraudulent communications.

NPCI works with participating banks and other ecosystem members to promote secure payment operations and improve awareness about digital payment fraud.

It is important to note that NPCI does not replace the police or the RBI. Its responsibilities relate to payment infrastructure and the operational framework of participating institutions.

Official website: National Payments Corporation of India

5.5 Police and Cyber Crime Investigation Units

State police departments and specialised cybercrime investigation units play a direct role in receiving complaints and investigating phishing and identity theft cases.

Their responsibilities include:

1. Registering complaints and taking appropriate legal action.

2. Identifying the persons responsible for fraudulent communications.

3. Tracing bank accounts and suspicious financial transactions.

4. Collecting electronic and documentary evidence.

5. Obtaining relevant information from banks, telecom operators and online platforms through lawful procedures.

6. Coordinating with other state and central agencies where necessary.

Since cybercriminals may operate from different locations, coordination between police departments is essential for effective investigation.

Chapter VI – Challenges in the Investigation and Enforcement of Phishing and Online

Identity Theft Laws

Although India has introduced several legal provisions to address cybercrime, the practical enforcement of these provisions continues to face difficulties. The following challenges are particularly significant.

6.1 Difficulty in Identifying the Actual Offender

One of the major challenges in phishing cases is identifying the person who actually committed the offence.

Fraudsters frequently use fake identities, temporary mobile numbers, false email addresses and multiple bank accounts. In some cases, the person whose bank account receives the money may only be a money mule and may not be the person who organised the phishing operation.

This makes it difficult for investigating authorities to identify the principal offender and establish the complete chain of transactions.

6.2 Anonymity and Use of Technology

Cybercriminals may use virtual private networks, proxy servers, fake websites and other technologies to conceal their identities and locations.

The use of such technologies can make it difficult to trace the source of fraudulent communications.

Further, some offenders operate through networks involving several intermediaries. Even when investigators identify one account or telephone number, tracing the actual individual behind the operation may require additional technical and financial investigation.

6.3 Jurisdictional Issues

Phishing is not necessarily restricted to one geographical location.

For example, a victim in Chennai may receive a fraudulent message originating from another state, while the money is transferred through a bank account located in a different state. The person operating the fraudulent website may even be located outside India.

This creates difficulties concerning the identification of the appropriate investigating authority, collection of evidence and coordination between different jurisdictions.

Although Section 75 of the IT Act provides for the extraterritorial application of the Act in specified circumstances, practical enforcement may depend on international cooperation, access to information and the availability of evidence.

6.4 Delay in Reporting Cyber Fraud

Time is extremely important in cases involving financial cyber fraud.

Once the victim transfers money, the amount may be moved through multiple accounts or withdrawn before the authorities receive information about the transaction.

Some victims delay reporting because they initially believe that the transaction will be reversed automatically. Others hesitate because of embarrassment or lack of awareness.

Such delays may reduce the possibility of freezing the funds and recovering the money.

6.5 Difficulties in Collecting and Preserving Electronic Evidence

Electronic evidence plays a major role in proving phishing and identity theft offences.

However, emails, messages, websites and digital transaction records may be deleted, modified or become inaccessible over time.

Investigators must establish the authenticity of the evidence and maintain an appropriate chain of custody.

The Bharatiya Sakshya Adhiniyam, 2023 prescribes requirements for electronic records. Failure to comply with the relevant evidentiary requirements may create difficulties during trial.

The Supreme Court's decision in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, demonstrates the importance of properly proving electronic records under the earlier Evidence Act framework.

6.6 Limited Awareness Among the General Public

A considerable number of phishing incidents occur because individuals are unaware of the methods used by cybercriminals.

Many people are unable to distinguish between genuine bank communications and fraudulent messages. Some individuals also believe that providing an OTP to a person claiming to be a bank representative is part of a normal verification process.

The lack of awareness is particularly concerning when fraudulent messages use familiar names, logos and official-looking language.

Therefore, cybersecurity education must be treated as an important part of cybercrime prevention.

6.7 Difficulties in Recovering Financial Losses

Registering a criminal complaint does not automatically result in the recovery of money lost through phishing.

Even when the offender is identified, the transferred amount may already have been withdrawn or moved through several accounts.

The victim may therefore face difficulties in obtaining financial relief despite the existence of criminal proceedings.

This highlights the need for stronger coordination between banks, payment service providers and law enforcement authorities.

6.8 Limited Coordination Between Institutions

Effective action against phishing requires cooperation between police departments, banks, telecom operators, online platforms and cybersecurity agencies.

However, delays in obtaining information or coordinating between different institutions may affect investigations.

The problem becomes more complicated when the offender operates across different states or countries.

A more organised system of information sharing and time-bound cooperation is therefore necessary.

6.9 Misuse of Artificial Intelligence and Emerging Technologies

The development of artificial intelligence has introduced additional challenges in identifying fraudulent communications.

Criminals may use AI-generated messages, voice imitation and manipulated images to impersonate trusted individuals.

For example, a person may receive a telephone call that appears to be from a relative or senior official requesting an urgent money transfer.

Such communications can be difficult to identify because they may resemble genuine conversations.

The existing legal framework must therefore be implemented in a manner that can address emerging technological methods without depending exclusively on traditional forms of evidence.

6.10 Psychological and Reputational Impact on Victims

The consequences of phishing are not limited to financial loss. Victims may experience fear, embarrassment and a loss of confidence in digital transactions.

In identity theft cases, an innocent individual may also be suspected of participating in fraudulent activities carried out by another person using their identity.

Victims may have to approach banks, police authorities and other institutions repeatedly to establish that they were not responsible for the fraudulent activity.

Therefore, an effective legal response must also consider victim assistance, privacy and reputational protection.

Chapter VII – Suggestions and Recommendations

Based on the above analysis, the following measures may help strengthen India's response to phishing and online identity theft.

7.1 Strengthening the Existing Legal Framework

The existing provisions of the Information Technology Act, 2000 provide an important foundation for addressing cyber fraud. However, the increasing sophistication of phishing methods requires continuous examination of whether the existing provisions and enforcement mechanisms remain adequate.

The law should be implemented in a manner that clearly addresses emerging methods of impersonation, digital identity misuse and technology-assisted financial fraud.

7.2 Improving Cybercrime Reporting Mechanisms

The National Cyber Crime Reporting Portal and the 1930 helpline should be made more accessible to individuals from different educational and linguistic backgrounds.

Awareness campaigns should explain the reporting procedure in regional languages. Victims should also receive clear information about the status of their complaints and the action taken by the concerned authorities.

7.3 Faster Coordination Between Banks and Police Authorities

Banks and law enforcement agencies should establish more efficient systems for sharing relevant information in financial cybercrime cases.

When a victim reports an unauthorised transaction, the concerned institutions should act promptly to examine the transaction and prevent further transfer of funds wherever possible.

A coordinated response system can improve the possibility of recovering money before it is withdrawn or transferred through multiple accounts.

7.4 Strengthening Customer Protection

Banks and payment service providers should continuously improve their fraud detection mechanisms.

They should introduce stronger transaction monitoring, unusual activity alerts, risk-based authentication and timely communication with customers.

Customers should also be provided with clear information about the circumstances in which they may be held liable for unauthorised transactions.

7.5 Improving Digital Literacy and Public Awareness

Digital literacy programmes should be conducted in educational institutions, workplaces and rural communities.

People must be educated about:

- The importance of keeping OTPs and passwords confidential.
- Identifying fraudulent banking messages.
- Avoiding unknown links and attachments.
- Recognising fake customer-care numbers.
- Reporting unauthorised financial transactions immediately.
- Using official websites and applications for financial services.

Public awareness should not be limited to occasional campaigns. It should become a continuous process.

7.6 Effective Implementation of Data Protection Principles

The DPDP Act and its Rules should be implemented according to their applicable commencement schedule.

Organisations handling personal information should adopt appropriate security safeguards and responsible data-handling practices. They should also establish effective grievance redressal mechanisms.

Where personal information is exposed due to a data breach, the responsible organisations should take appropriate steps under the applicable legal framework to prevent further misuse.

7.7 Strengthening International Cooperation

Since phishing operations may involve offenders and digital infrastructure located outside India, international cooperation is essential.

India should strengthen cooperation with foreign law enforcement agencies and relevant international organisations to facilitate lawful information sharing, preservation of digital evidence and investigation of cross-border cyber offences.

7.8 Training and Capacity Building for Investigating Authorities

Cybercrime investigation requires technical knowledge and specialised training.

Police officers, prosecutors and judicial officers should receive regular training on digital evidence, financial transaction tracing, cyber forensics and emerging forms of online impersonation.

Specialised cybercrime investigation units should also be strengthened with appropriate technical resources.

7.9 Improving Victim Assistance and Financial Recovery

Victims should be provided with clear guidance regarding the procedure for reporting fraud, contacting banks, preserving evidence and seeking appropriate legal remedies.

A more effective grievance redressal system should be developed to ensure that victims do not have to approach multiple authorities without receiving proper assistance.

The possibility of recovering financial losses should also be improved through faster coordination and better monitoring of suspicious transactions.

7.10 Responsible Use of Artificial Intelligence in Cybersecurity

Financial institutions and cybersecurity agencies should make use of suitable technological tools to identify suspicious communications, unusual transactions and patterns of fraudulent activity.

At the same time, the use of automated detection systems should be subject to appropriate safeguards to prevent errors and protect the privacy of legitimate users.

Chapter VIII – Findings and Conclusion

8.1 Findings of the Study

The present study identifies the following important findings:

1. Phishing and online identity theft are closely connected cyber offences, as phishing is frequently used as a method of obtaining personal information that is subsequently misused for identity theft.

2. The Information Technology Act, 2000 provides specific legal provisions to address identity theft and cheating by personation through computer resources, particularly Sections 66C and 66D.

3. The Bharatiya Nyaya Sanhita, 2023 supplements the cybercrime framework by addressing cheating and personation under Sections 318 and 319.

4. Although several legal remedies are available, victims often experience difficulties in identifying the actual offenders because cybercriminals operate through anonymous accounts, fake identities and multiple financial intermediaries.

5. Delay in reporting fraudulent transactions affects the possibility of freezing transferred funds and recovering financial losses.

6. The RBI's customer protection framework provides important safeguards against unauthorised electronic banking transactions. However, the liability of customers depends on the circumstances of each transaction and the applicable regulatory directions.

7. Electronic evidence is essential for prosecuting phishing and identity theft cases. Difficulties relating to the collection, preservation and admissibility of such evidence may affect the outcome of criminal proceedings.

8. The National Cyber Crime Reporting Portal, 1930 helpline, CERT-In and I4C play important roles in preventing and responding to cybercrime.

9. The Digital Personal Data Protection Act, 2023 provides a broader framework for protecting personal information, but its substantive provisions must be considered in accordance with their phased commencement.

10. Greater public awareness, institutional coordination, technological safeguards and victim-oriented remedies are necessary to improve the effectiveness of India's cybercrime prevention framework.

8.2 Conclusion

The development of digital technology has made communication and financial transactions easier, but it has also created new opportunities for cybercriminals to exploit individuals.

Phishing and online identity theft have emerged as serious threats because they affect not only the financial security of individuals but also their privacy, dignity and personal identity. What makes these offences particularly concerning is that they are often committed through deception, making it difficult for ordinary individuals to identify fraudulent communications before suffering a loss.

The present study shows that India has established a legal framework to address these offences through the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023.

Provisions such as Sections 66C and 66D of the IT Act provide specific punishment for identity theft and cheating by personation through computer resources. Similarly, Sections 318 and 319

of the BNS address cheating and impersonation. The DPDP Act, 2023 further recognises the importance of protecting personal information and regulating its processing, subject to its phased commencement.

However, the existence of legal provisions does not necessarily guarantee effective protection.

Victims continue to face difficulties in reporting cyber fraud, recovering lost money and obtaining timely assistance. The anonymity of offenders, cross-border transactions, lack of technical resources and difficulties in preserving electronic evidence create considerable obstacles to investigation and prosecution. In many situations, the financial consequences are immediate, whereas the legal process may take considerable time.

Therefore, addressing phishing and online identity theft requires more than introducing stricter punishments. There must be a practical system through which victims can report offences easily, banks can respond quickly and investigating authorities can obtain relevant information without unnecessary delay. Public awareness and digital literacy must also receive greater attention, as individuals should be able to recognise suspicious communications and understand how their personal information can be misused.

Ultimately, the effectiveness of India's legal framework should be measured not merely by the number of offences covered under legislation but also by the extent to which individuals are protected in practice. A combination of effective legal enforcement, responsible handling of personal data, stronger institutional cooperation and accessible victim remedies is essential to create a safer digital environment. Protecting an individual's online identity should be treated as an important part of protecting their privacy, dignity and fundamental rights in an increasingly digital society.

References and Bibliography

The following references are arranged in a legal research-paper format. Statutes and judicial decisions are given in a Bluebook-style format, followed by official regulatory materials and secondary references.

I. Statutes and Legislative Materials

1. The Constitution of India, 1950.

2. The Information Technology Act, No. 21 of 2000, India Code (2000).

3. The Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009).

4. The Consumer Protection Act, No. 35 of 2019, India Code (2019).

5. The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

6. The Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).

7. The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).

8. The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

II. Judicial Decisions

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

3. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

4. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

III. Government and Regulatory Materials

1. Reserve Bank of India, Customer Protection – Limiting Liability of Customers in

Unauthorised Electronic Banking Transactions, RBI/2017-18/15,

DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017).

2. Indian Computer Emergency Response Team, Ministry of Electronics and Information

Technology, Directions under Sub-section (6) of Section 70B of the Information Technology Act,

2000 (Apr. 28, 2022).

3. Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), official website.

4. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025 (Nov. 2025).

5. Reserve Bank of India, Reserve Bank of India (Commercial Banks – Responsible Business Conduct) Directions, 2025, as amended in 2026.

6. National Cyber Crime Reporting Portal, Government of India, available at https://cybercrime.gov.in/.