International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 14, Issue 12, December 2025)

Concept, Techniques and Goals of Phishing : A Legal Perspective

Ishita Singh
Ph.D. Research Scholar (Law) Mahakaushal, University, Jabalpur, India

A deceptive way where sensitive information like usernames, passwords, credit /debit card details, bank account information or other important personal data is stolen by masquerading as a reputable source by providing tempting offers to victims in order to deceive them, exactly like a fisherman uses bait to catch a fish. It is a fraudulent techniques used by cybercriminals, derived from the analogy of "fishing" for sensitive data. It is one of the most prolific and evolving forms of cybercrime. It is executed through email spoofing, fake websites, SMS (smishing), voice calls (Vishing) and social media impersonation. Phishing attacks are no longer limited to naive individuals, they now target employees of large corporations, law enforcement agencies, banks and governments department.

India has seen one exponential increase in phishing related crimes. According to the Indian Computer Emergency Response Team India handled over 13 lakh cyber incidents in 2023 alone, a significant number of which involved phishing attacks.

The National Crime Record Bureau (NCRB) also reported a consistent rise in cyber fraud cases over the first few years, with a steep increase post- 2020. This coincides with the COVID-19 pandemic, which drove unprecedented dependence on digital systems, remote work, online banking and e-governance, thereby enlarging the attack, surface for cyber criminals.

Moreover, phishing has evolved significantly from simple, grammatically incorrect emails to sophisticated campaigns that use artificial intelligence (AI) to mimic voice, generate realistic fake websites and even automate targeted attacks. Such developments render conventional legal tools and enforcement mechanisms ineffective or insufficient while phishing is inherently technical, its consequences are deeply legal: identity theft, financial fraud, date breaches and violations of privacy and contractual obligation.

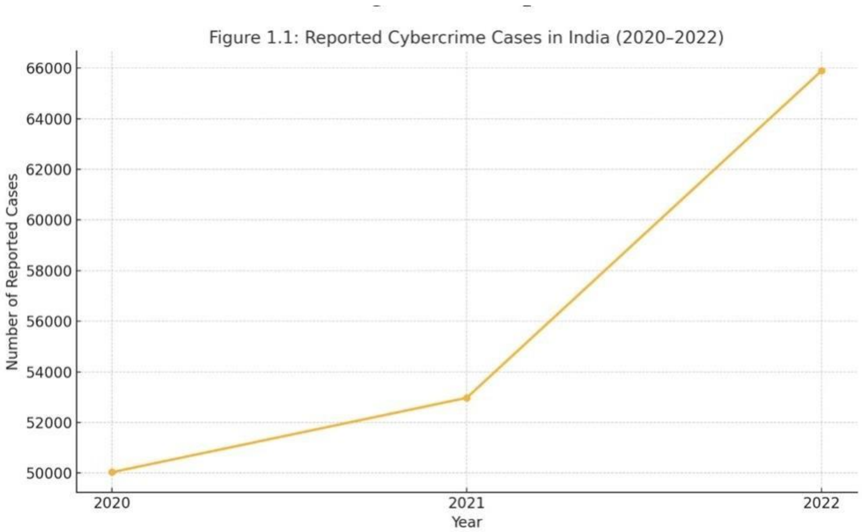


Figure 1.1: Reported Cybercrime Cases in India (2020–2022) based on real data from NCRB.

I. Working Mechanism

- *Impersonation:*

  Cyber criminals pretend to be from a reputed organization or legitimate people.

- *Deception:*

  They deceive victims pretending to be legitimate people or groups via sending messages, emails, texts, phone calls with urgent requests or with luring offer and deals.

- *Social Engineering:*

  Exploit people's trust and urgency to manipulate victims.

II. Tactics

- Finding, purchasing or **scraping** known contact information.
- Creating fake websites imitating the original ones.
- Using techniques like **DNS fast fluxing** to disguise their services.
- Using **domain and email spoofing** to look their messages to be legitimate.
- Manipulating links so that URL looks original and correct.
- Sending emails from trusted infrastructure so that mails don't go to the **spam** and get past spam filters.
- Using **generative AI** to create realistic sounding and ever free messages.

III. Latest Phishing Scams & Techniques:

Website forgery Scam

In this type of phishing the cybercriminal creates a websites exactly identical to the original websites, such as a bank where when opened by a user, via a hyperlink inside a forum, via a search engine, the victims opens a website which the user feels and looks to be original and legitimate site instead of the fraudulent copy. The information then entered by the user is stored for sale or other illegal and malicious use.

Previously the fake websites used to be easily spotted due to their shoddy craftsmanship but today the cybercriminals make a picture perfect representation of the original. It is possible to spot a fraud by checking the URL in the web browser.

If the page is trusted as insecure and HTTPs is not on, it is a red flag and guarantees either the site is broken or it is a phishing attack.

Account deactivation Scam:

By urgent emails, messages, phone calls through a cybercriminal making the victim behave that their account of their is going to be deactivated, criminals trick victims to pass on their sensitive data like username, passwords, OTPs to them or by sending the victims a fake links created by them to be opened by the victims where when they provide their data, its collected by them for malicious illegal activity. This type of scam can be checked by directly going to the website in question and checking if the legitimate provider notifies the user of the same urgent deactivation.

Advanced Fee Scam:

It is email type phishing popularly known as "Nigerian Prince email" where on alleged Nigerian Prince in a desperate situation offer the victim to give them large amount of money for a small amount of price as "Fee". When the fee is paid by the victim, no money come in the bank account of the victim. Surprisingly this type of scam is prevalent in different forms for one hundred years. It was originally known as the Spanish provider in 1800s.

Spear Phishing:

This type of phishing targets a specific individual or company, hence the term being "Spear phishing", by collecting information about that individual or company, being a personalized scam, being most effective type.

Clone Phishing:

It involves mimicking a legitimate mail previously delivered to a person and modifying its links or attached files to deceive and trick the victim to open a malicious website or file. Eg: taking an email and attacking malicious file and resending the mail with a spoofed email address that looks to come from original sender.

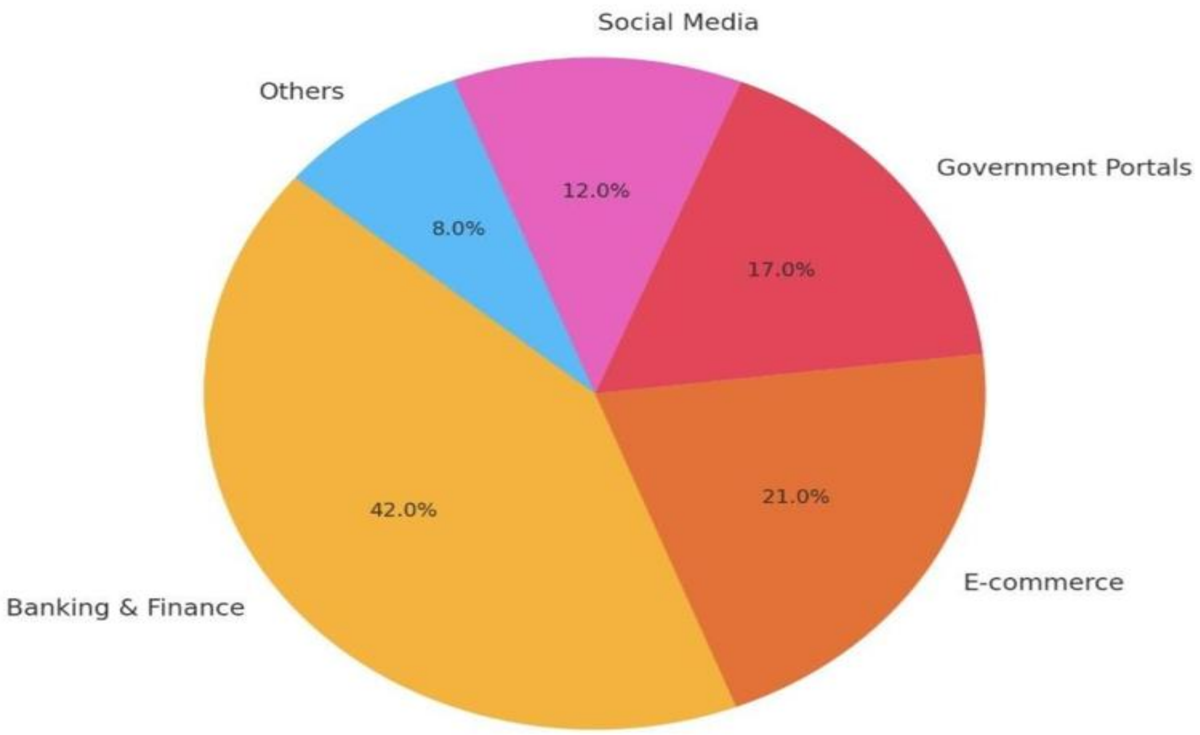
Whaling:

This type of phishing specially attacking senior executives or privileged uses within business, thus the term "Whaling" likely to require attention of the person such as legal subpoenas or other example is whaling emails scam that appear to come from a privilege authority or executive. Eg. email from a CEO to their subordinate asking for help in the form of transferring money to them. Lower level employees generally gets fooled by this type of phishing.

IV. Role Of Phishing In India

The expansion of digital services in India over the past decade has been accompanied by an alarming rise in cybercrime, generally phishing related fraud. Being one of the fastest growing internet economies, India saw its user base swell to over 850 million by 2023, creating a vast digital population vulnerable to exploitation. Phishing not only offers a low-cost, high-reach avenue to commit financial fraud, but also thrives in the absence of widespread digital literacy and a lack of cohesive legal deterrence.

Figure 1.4: Sector-wise Distribution of Phishing Attacks in India (2023)



Adequacy, Implementation and Reform of legal frameworks dealing with phishing in India.

1. How effective is the current Indian legal framework in addressing phishing as a cybercrime?

This central question seeks to evaluate whether existing laws- primarily the Information Technology Act, 2000, and the Indian Penal Code- provide sufficient coverage, precision, and deterrence for phishing-related offences. The sub-questions here include:

- Are existing provisions, such as Sections 66C and 66D of the IT Act, adequate to prosecute modern phishing techniques?
- Does the current legal framework address new modalities of Phishing, including voice phishing (vishing), SMS-based scams (smishing), and website cloning?
- How do Indian courts interpret and apply cybercrime laws to phishing cases?

The analysis will consider both the statutory scope and judicial application of these laws in reported cases across various states.

2. What are the major institutional and enforcement challenges in combating phishing in India?

This question explores the capacity, coordination, and limitations of India's institutional machinery in detecting, investigating, and prosecuting phishing crimes. It addresses:

- The role and effectiveness of key bodies such as CERT-In, state cybercrime cells, RBI, and law enforcement agencies.
- Gaps in cyber forensic capabilities and digital evidence handling.

- Issues with FIR registration, cross-jurisdictional coordination, and inter-agency delays.
- Lack of training and cyber awareness among frontline police and judicial officers.

This inquiry draws from real case studies (such as the Axis Bank vishing scam and CoWIN phishing attack) to understand how fragmented or reactive enforcement weakens phishing prevention efforts.

3. How does India's approach to phishing regulation and prosecution compare with global best practices?

Phishing is an inherently transnational crime, with attackers often operating from foreign jurisdictions using globally distributed infrastructure. This question places India in a comparative legal context, examining how other jurisdictions-such as the United States, the European Union, Singapore, and Australia- have enacted specific anti-phishing laws or regulatory frameworks. It explores:

- Whether India should become a signatory to the Budapest Convention on Cybercrime.
- How bilateral treaties, MLATs (Mutual Legal Assistance Treaties), or cyber diplomacy can improve India's cross-border prosecution of phishing.
- What lessons can be learned from models such as the U.S. Computer Fraud and Abuse Act (CFAA) or the EU's GDPR in terms of data protection and victim rights.

The objective here is to identify actionable insights and benchmarks for **legislative and procedural harmonization.**

4. What legal and policy reforms are necessary to improve India's response to phishing crimes?

Building on the gaps identified in the previous questions, this inquiry focuses on forward-looking reforms. It examines:

- Whether India needs a dedicated anti-phishing statute or amendments to the IT Act with more specific provisions.
- Mechanisms to empower CERT-In and the Ministry of Electronics and IT with real-time takedown and domain-blocking powers.
- Introduction of a victim compensation framework, including a Financial Cyber fraud Victim Fund as seen in some OECD countries.
- Need for integrated cyber training for judges, prosecutors, and investigating officers.

This question will also address public awareness mechanisms, such as mandated phishing simulations in workplaces, inclusion of cyber security in school curricula, and public campaigns in regional languages.

V. Key Legal And Institutional Challenges:

1. *Domain Spoofing and Absence of Legal Recognition:* Domain spoofing was central to the scam. However, Indian law does not currently criminalize domain name impersonation explicitly. While Sections 66C and 66D of the IT Act were used, no targeted statute addressed fake domain registration with criminal intent.
2. *CERT-In Intervention:* CERT-In issued an advisory and began blacklisting known fake domains. However, takedown requests had to go through foreign hosting services and registrars, many of whom responded slowly or refused cooperation citing local privacy laws. This exposed India's dependence on external service providers for mitigation.
3. *National Security Implications:* The breach of health-related data raised concerns about national security and data privacy. Experts noted that stolen CoWIN credentials could be used for identity fraud, financial scams, and even political manipulation (e.g., through mass SMS campaigns using stolen contact data).
4. *Public Awareness Failure:* The Ministry of Health and Family Welfare issued alerts, but these were mostly confined to English- language websites and social media. In rural areas, awareness was nearly absent, and many victims fell for the scam without ever knowing they were defrauded.
5. *Investigative Inertia:* FIRs were filed across Delhi, Maharashtra, and Karnataka. However, no arrests were made in connection with the domain fraud due to lack of access to WHOIS data and absence of cyber diplomacy protocols to trace buyers.

VI. Consequences And Broader Implications:

a. Data security in government-run digital services came under the spotlight, with concerns raised about the CoWIN platform's own API being vulnerable.

b. The phishing campaign led to a parliamentary question about India's cyber readiness in March 2022, to which the ministry of Electronics and IT admitted "limited jurisdiction" in prosecuting such global scams.

c. Cyber security analysts warned that similar attacks could be deployed against other digital services like DigiLocker, GST, or PM-Kisan.

This case highlights how phishing is no longer limited to private or financial fraud- it now extends to state platforms, where implications are both national and constitutional.

It strengthens the argument that phishing legislation must include specific provisions on impersonation of government domains, mandate rapid takedown protocols, and empower CERT-In with direct enforcement capacity in cyber infrastructure protection.

VII. What Is Needed:

The increasing digitalization of India's public and private sectors has transformed the country into one of the largest and most dynamic digital economies in the world. While this transformation has brought substantial benefits, including improved governance, financial inclusion and access to services, it has also led to an unprecedented rise in cyber vulnerabilities, phishing being one of the most common and destructive among them.

1. Legal and Academic Relevance

- Despite the growing number in phishing cases reported across India, there is a conspicuous gap in legal literature and academic research focusing specifically on phishing as a distant form of cybercrime. Most scholarly works broadly address cybercrime or data protection but fail to explore phishing in detail from a doctrine, comparative and enforcement perspective.
- Should provide a comprehensive legal analysis of phishing related provisions under Indian statutes.
- Critically evaluating judicial decision and enforcement practices.
- Bringing the literature gap by positioning phishing as a distinct subject requiring targeted legal attention.
- Offering a structured and evidence backed legal reform framework suitable for policy makers, law students and scholars of cyber law.

2. Institutional Significance:

- CERT-In, which monitors cyber threats and incident responses.
- Law Enforcement agencies, particularly cybercrime cells at the state and district level.
- Regulatory Bodies like the Reserve Bank of India (RBI), SEBI, Ministry of electronics and Information Technology (MeitY).
- Judiciary, which is increasingly confronted with phishing, related disputes involving identity theft, financial fraud and data misuse.

3. Policy and Governance Import:

For National Cyber security policy, digital payments regulation and consumer Protection frameworks, it can inform:-

- The drafting of amendments to the Information Technology Act 2000.
- Development of a centralized phishing complaint and redressal mechanism.
- Implementation of stricter KYC and SIM issuance norms under Telecom regulations.
- Adoption of global cybercrime treaties or bilateral mutual legal Assistance Treaties (MLATs).

4. Protection of Citizen Rights and Financial Security

Phishing crimes directly undermine fundamental rights such as the right to privacy (Article 21 of the Constitution), the right to information, and the right to property (Article 300A). Victims often lose their life savings, suffer reputational damage, or face prolonged legal and bureaucratic hurdles in seeking redress.

This study proposes:

- Legal safeguards for victims of digital financial fraud.
- Enhanced liability provisions for intermediaries are digital service providers.
- Inclusion of phishing under victim compensation schemes and fast- track grievance redressal mechanisms.

By doing so, the research enhances citizen protection and digital trust-essential elements for India's sustainable digital development.

5. Enhancing Cyber Awareness and Digital Resilience

One of the major factors contributing to phishing success is low awareness among users, particularly in rural and semi-urban areas. The study highlights the importance of:

- Launching targeted cyber hygiene campaigns.
- Integrating cyber security education into school and university curricula.
- Encouraging organizations to adopt phishing simulation tools and employee training.

REFERENCES:

[1] 'Cyber security And Cybercrime in India' by Dr. Anurag Kumar Srivastava, Prashant Kumar Chauhan.

[2] 'Cybercrime in India' by Dr. Deepti Meena, Dr. Sarita Dehariye Mehra.

[3] 'Phishing Attack: A complete Guide', e-book by Gerardus Blokdyh.

[4] 'Phishing Dark Waters: The offensive And Defensive Sides of a Malicious Emails' by Wiley.

[5] https://www.phishing.com

[6] National cyber Security Centre http://www.ncsc.gov.in

[7] http://sancharsaathi.gov.in