International Journal of Law, Justice and Jurisprudence

E-ISSN: 2790-0681
P-ISSN: 2790-0673
Impact Factor: RJIF: 5.67
www.lawjournal.info
IJLJJ 2025; 5(2): 259-262
Received: 25-06-2025
Accepted: 29-07-2025

Dr. Shashirekha Malagi
Senior Assistant Professor of Law, Karnatak University's Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka, India

Correspondence Author:
Dr. Shashirekha Malagi
Senior Assistant Professor of Law, Karnatak University's Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka, India

The concept of phishing on cyber space: The special reference to the Indian law & judiciary

Shashirekha Malagi

DOI: https://dx.doi.org/10.22271/2790-0673.2025.v5.i2c.240

Abstract
In the era of information technology, the rapid growth of internet usage and mobile technology has opened new frontiers, not just for innovation and communication, but also for crime. One of the most dangerous and rapidly evolving cybercrime is phishing. Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies. Hence, a doctrinal study was carried out to focus on the growing number of reported cases on phishing. Phishing is not just a technical issues but which is a legal one. In India, multiple laws and authorities address phishing, even though there isn't a single, dedicated "anti-phishing" statute in India. The need is not only to have appropriate legal provisions for phishing on cyber space but also to create awareness among the general public and strict functioning of law enforcement agencies.

Keywords: Phishing, The Information Technology Act 2000, Judiciary, law enforcement agencies

Introduction
In today's interconnected digital world, phishing has emerged as one of the most common and dangerous forms of cybercrime. As India rapidly moves toward digital inclusion through initiatives like UPI, Digital India, Aadhaar linked services, the threat of phishing looms larger than ever. Nowadays Phishing is slowly evolving and fraudsters are certainly adapting to security controls and improving their level of sophistication. Phishes are wary of relying solely on the human factor and are less willing to wait for users to enter their data. Instead, malicious users are now sending out malicious emails seeded with Trojans that steal usernames and passwords, including for online banking accounts. This article explores the concept of phishing, its impact in India, and how Indian cyber laws attempt to counter this evolving threat.

Meaning of Phishing
The term "Phishing" is not directly defined by the Indian Laws. However, phishing activities are recognized as cybercrimes and are prosecuted under various sections of the Information Technology Act2000.
Phishing is a type of cyber attack in which attackers impersonate legitimate individuals or organization typically through emails, messaging apps, websites, or phone calls to trick victims into revealing sensitive information, such as

- Login credentials (e.g. username and p-assword)
- Bank account or credit card numbers
- Personal identity details (e.g. Aadhaar number, Pan SSN)
- One time passwords (OTPs)or two factor authentication (2FA) Codes

Phishing is an illegal act whereby fraudulently sensitive information is acquired, such as passwords and credit card details, by a person/entity by misrepresenting himself as a trustworthy person or business in an official electronic communication, such as email or instantaneous communication. Therefore, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit cards. Theses communications purporting to be from popular social websites, auction sites, online payment processors, or IT Administrators are commonly used to lure the unsuspecting. Phishing is typically carried out by email or instant messaging and it often directs users to

enter details at a fake website whose look and feel are almost identical to the legitimate one [1].

Example
An SMS claiming to be from your bank says, "your account will be blocked. Click here to verify". The link leads to fake page steals your credentials.

Case Study
In 2020, a fake government website offering COVID relief asked users to enter their Aadhaar and bank details. Thousands of citizens lost money to this phishing operation.
The National Association of software and service company v Ajay Sood [2]. In the year 2025 the Indian judiciary system has interpreted "phishing", in this case plaintiff has filed the present suit inter alia praying for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent E-mails purposely organizing from the plaintiff of using the trademark "NASSCOM" or any other mark confusingly similar in relation to goods or services. Here defendant is using the trademark of the plaintiff and sending mails to the customers giving the impression that mail was sent by NASSCOM.
It was held by the court that, "Phishing" is a form of internet fraud. In case of "phishing", a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords, etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party.
Typically "Phishing" scams involve persons who pretend to present online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details [3].

The different forms of Phishing as follows:

- Spear Phishing: A targeted attack aimed at a specific individuals or organization, often using personalized information.
- Smishing and Vishing: Phishing attempts carried out via SMS (smishing) or voice calls(vishing).
- Clone Phishing: Attackers create a nearly identical replica of a legitimate email to trick users.
- Pharming: Redirecting users from a legitimate website to a fake one without their knowledge.
- Email Phishing: Fake emails or websites that mimic legitimate sources (bank, government portals), The most common type, where attackers send mass emails appearing to be from reputable sources.

The Provisions under the Information Technology Act 2000
The phishing is covered under the Information Technology Act 2000 as follows:

1. Section 43 of the Information Technology Act deals with penalty for download, damage, etc., without the consent: If any person without the permission of the owner of the computer, computer system, computer network, accesses, downloads, intreoduces, disrupts, denies, or provides any assistance to other people can held liable to pay penalty under this section [4].
2. The Section 66 of the Information Technology Act 2000: Computer related offences, If the accounts of a victim are compromised by the phisher, who does any act mentioned in Section 43 of the Information technology Act, shall be imprisoned for a term which may exceed up to three years or with a fine which may exceed up to five lakh rupees or both [5].
3. **Section 66c of The information technology Act 2000 deals with theft of indenty:** This provision prohibits the use of electronic signatures, passwords, and any other feature which is a unique identification of a person. Phishers disguise and portrary themselves as the true owners of the accounts and perform fraudulent acts [6].
4. **The Section 66D of the Information Technology Act 2000 deals with cheating by personation:** The provision provides punishment for cheating by personating using communication devices or computer sources. Fraudsters use URLs that contain the link for a fake website of banks and organizations and personate themselves as the bank or the financial institution [7].

Explanation
All the provisions of the Information Technology Act 2000 which are relevant to the phishing scams are bailable offences as per under Section 77B of the? Information Technology Act 2000(Amendments 2008). This is because of the uncertainty as to who the real criminal is. There is always translucent screen in front of the phisher which hides their identity and there may be cases wherein the wrong person is convicted for a crime that they have never committed, due to which the offense under these Section is made bailable. Phishing is also an offence under various Sections of the BNS, ie., Cheating (Section 415), Mischief (Section 425), Forgery (Section 464), and Abetment (Section 107) [8].

Judicial Response
India's growing internet user base expected to cross 9oo million by 2025, makes it fertile ground for cyber criminals. Phishing scams have been widely reported across:

- Banking and finance (e.g., SBI HDFC,UPI frauds)
- E-Commerce platforms (e.g., Amazon, Flipkart scams)
- Covid-19 and vaccine related phishing
- Government subsidy and tax refund scams
- Indian courts have taken phishing seriously, especially when it leads to significant financial loss or data compromise. In several cases, courts have upheld the application of IT Act 2000 sections along with BNS provisions to ensure strict punishment in India.

[1] Ramjee vPrasad & Vandana Rohokale, "Phishing in Cyber Security: The Lifeline of Information and Communication Technology,1st edition,2020, Springer cham, p33-42
[2] 2005 (30) PTC 437 Del.
[3] Gunikhan Sonowal, "Phishing and Communication Channels: A Guide to Identifing and Mitigating Phishing Attacks", Apress, Berkeley, ISBN: 978-1484277447
[4] Section 43 of the Information Technology Act
[5] The Section 66 of the Information Technology Act 2000
[6] Section 66c of 7the information technology Act 2000
[7] The Section 66D of the Information Technology Act 2000
[8] The provisions of Bharatiya Nyaya Sanhita, 2023.

Cases on Phishing [9]

In NASSCOM v. Ajay soad & othrs.[10]In this case it was recognized as a landmark on phishing, where defendants impersonated NASSCOM (National Association of software and service companies by sending fraudulent emails to extract personal data, much like modern phishing attacks. it was held that phishing was legally defined as "a form of internet fraud", impersonates a legitimate association to extract personal data". The court granted an interim injunction to stop misuses of NASSCOM's name and awarded Rs. 16 lakha in damages, high lighting that intangible harm (like reputational damage) qualifies for compensation.

The Punjab National Bank v. Poona Auto Ancillaries Pvt. Ltd. [11] In this case it was addressed about phishing incident involving a loss of over Rs.45 Lakha due to cybercrime. The court highlighted specialized cybercrime training for police personnel

In 2020 the Allahabad High Court in *Achin Sharma and 2 Others v. State of UP* held that the Legislature has inserted Section 66-D of the Information Technology (Amendment) Act 2000 with the view to provide an explicit deterrent against the growing occurrence of cheating by impersonating, also popularly referred to as "phishing". Phishing is today one of the most dangerous frauds. With the insertion of Section 66-D, phishing in addition to a civil contravention also becomes a penal offence according to the Information Technology Act 2000 [12].

In 2018 a New York man pleaded guilty to defrauding a national trade association out of more than $1.1 million in an email phishing scam and was awarded a maximum penalty of 20 years in prison [13].

Anti Phishing Initiatives [14]

Presently various strategies are being adopted nowadays to combat phishing, including the drafting of specific legislation and devising special technology targeted to tackle phishing.

- Technology based anti phishing strategies.
- Training users on how to identify and deal with phishing attemts.
- Use of anti phishing software programs: The programs work by identifying phishing content on websites band emails.
- Use of spam filters which also help protect users from phishers,
- Some organizations have introduced unique verification tools like challenge questions, secret images that serve the purpose of a verification password.
- Be cautious with emails and links, Always ckeck the sender's email address and be wary of messages with urgent language, unfamiliar greetings, or spelling errors. Avoid clicking on suspicious links or downloading unexpected attachments.
- Verify the source, if you recive a message from a bank, company or government agency asking for personal information, contact the organization directly using official contact details.
- Use Multi Factor Authemtication, even if a password is compromised, MFA adds an addition layer of protection, making it harder for attackers to gain accesss.
- Install Security Software, use anivirus software, firewalls, and anti-phishing toolbars to detect and block phishing threats.
- Keep systems updated, ensure your operating system, browser, and apps are regulary updated with the latest security patches.
- Monitor Accounts, regularly check bank and credit card statements for unauthorized transactions.

Also some of the law enforcement and regulatory bodies are working on phishing i.e. Indian Cyber Crime Coordination Centre, CERT-Issues alerts on phishing attacks and cyber threats, Cyber Crime Police Cells, National Cyber Crime Reporting Portal-A centralized portal to report phishing and other cyber crimes. RBI Guidelines mandate two-factor authentication and customer education for nanks.

The Challenges in Enforcement against Phishing in India as follows

- Lack of Specific Law-The India lacks a comprehensive specific law on phishing.
- Digital Evidence handling-Requires skilled personnel and forensic tools.
- Jurisdictional issues-Phishing often involves international actors, making investigation and prosecution complex.
- No awareness-Many victims don't recognize phishing or awareness to report the case.

The Importance of Public Awareness

- Preventing phishing isn't just a matter of technology-education and awareness are key. Many successful phishing attacks exploit human error rather than software vulnerabilities. Therefore, spreading awareness can significantly reduce the chances of falling victim.
- Educational Campaigns: Governments, schools and organizations should run regular cyber security awareness programs.
- Cyber security in the school curriculum: Including basic internet safety and phishing awareness in school curriculums.
- Simulated Phishing Tests: Business can conduct fake phishing drills to train employees in recognizing phishing attempts.
- Media Outreach: Using TV, radio, social media, and online platforms to inform the public about common phishing tactics.

Best Practices for Individuals

- Never click on suspicious links or download unknown attachments
- Always check the sender's email ID or phone number
- Avoid sharing OTPs or passwords, even with those

[9] Prof. (Dr)Jyoti Rattan, "Cyber Laws, Information Technology & Artificial Intelligence", 10th edition, 2024, New Delhi-Bharat Law House Pvt. Ltd. p-657

[10] Delhi High court, March 2005.

[11] Bombay High Court 2018.

[12] Criminal Misc.writ Petition No.-5755 of 2020.

[13] *Ibid.*

[14] Prajwal D'Souza, DH Special on Cybercrime Conviction rate dismal. 23%, Hubballi-Dharwad, Friday, August 22, 2025, pages 16, Vol 37, No 233

claiming to be “officials”
- Use strong, unique passwords and enable 2FA (Two Factor Authentication)
- Report phishing attempts immediately to your bank and at cybercrime.gov.in.

Conclusion

Combating phishing is not just a legal necessity but a foundational requirement for a secure digital India. But India does not have a specific statute that exclusively deals with phishing, existing provisions under the Information Technology Act2000 and BNS provide only legal remedies but which is not sufficient in the present situation. As phishing grows more sophisticated, it is crucial for legal frameworks, enforcement mechanisms and public awareness to evolve simultaneously.

References

1. The Information Technology Act 2000
2. The BNS
3. The Ministry of Electronics and Information Technology
4. CERT-In Advisories
5. The Supreme court &High Court judgments on cybercrime