International Journal of Information Movement *Vol. 9 Issue V* *(September 2024)*
Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 21-25**

COMBATTING PHISHING IN CYBERSPACE: INSIGHTS FROM INDIAN LAW AND THE JUDICIARY

Dr. D B Ravikumar
Assistant Professor
Saraswathi Law College, Chitradurga district, Karnataka state, India
Email-id :- dr.ravikumar5066@gmail.com

Abstract: In the age of information technology, the swift increase in internet usage and mobile technology has created new opportunities, not only for innovation and communication but also for criminal activities. One of the most perilous and swiftly changing forms of cybercrime is phishing. Phishing exemplifies social engineering tactics designed to deceive users and takes advantage of the inadequate usability of existing web security technologies. Consequently, a doctrinal study was conducted to examine the rising number of reported phishing incidents. Phishing is not merely a technical concern but also a legal one. In India, various laws and authorities tackle phishing, despite the absence of a singular, dedicated 'anti-phishing' law. It is essential not only to establish suitable legal measures for phishing in cyberspace but also to raise awareness among the public and ensure the effective operation of law enforcement agencies.

Keywords : Anti-phishing, IT, Phishing, Law and Judiciary, cyber space and Law enforcement agencies

1.0 Introduction

Phishing stands out as a top cybercrime in our linked online space. It tricks people into giving away private details like login info or bank numbers. This scam hurts millions each year. In India, the push for more online services makes it riskier. Programs like UPI let users pay with phones in seconds. Digital India aims to connect every village to the web. Aadhaar ties IDs to services with a simple scan. These steps open doors to easy living but also invite attacks. Scammers target them hard. Fraudsters now change their tricks fast. They beat basic defenses and get smarter each time. Early phishing relied on fake emails or sites that fooled users into typing details. People fell for urgent alerts from "banks" or "government offices." But now, crooks avoid waiting for clicks. They know users learn to spot bad links. So, these bad actors send emails packed with hidden threats. Trojans hide inside attachments or downloads. Once opened, they grab passwords without a sound. This hits online bank accounts most. A quick example: An email looks like a UPI alert about a failed payment. It urges you to check a file. That file runs the Trojan and steals your login.

Such attacks spread wide in India. Reports show thousands of cases monthly, with losses in crores. Banks and police see a rise in stolen funds from these schemes. Why does it matter? It shakes trust in digital tools. Folks hesitate to use apps or share data. Yet, the need grows with more e-services. Indian laws fight back. The IT Act covers cyber fraud with fines and jail time. Rules demand banks to spot and stop scams. Police units track these crimes nationwide. Still, the threat shifts quick. Laws update to match, but gaps remain. This piece digs into phishing basics. It looks at harms in India. And it checks how rules try to block these growing dangers.

1.1 Meaning of Phishing: The term "Phishing" is not explicitly defined in Indian Laws. Nevertheless, phishing activities are acknowledged as cybercrimes and are subject to prosecution under different sections of the Information.

2.0 Technology Act 2000

Phishing refers to a form of cyber attack where attackers pose as legitimate individuals or organizations, usually via emails, messaging applications, websites, or phone calls, to deceive victims into disclosing sensitive information, including:

i. Login credentials (e.g., username and password)
ii. Bank account or credit card numbers
iii. Personal identity information (e.g., Aadhaar number, PAN SSN)
iv. One-time passwords (OTPs) or two-factor authentication (2FA) codes.

Phishing is an unlawful act in which sensitive information, such as passwords and credit card details, is fraudulently obtained by an individual or entity misrepresenting themselves as a trustworthy person or business through official electronic communications, like emails or instant messages. Thus, phishing constitutes a criminally fraudulent attempt to obtain sensitive information, including usernames, passwords, and credit card details. These communications, which claim to be from well-known social media platforms, auction sites, online payment processors, or IT administrators, are frequently used to entice unsuspecting individuals. Phishing is usually executed through email or instant messaging and often leads users to input their information on a counterfeit website that closely resembles the legitimate one.

2.1 Example: An SMS purporting to be from your bank states, "your account will be blocked. Click here to verify." The link directs you to a fraudulent page that steals your credentials. Case Study. In 2020, a counterfeit government website promising COVID relief requested users to provide their Aadhaar and bank information. This phishing scheme resulted in significant financial losses for thousands of citizens. The National Association of Software and Service Companies v. Ajay Sood. In 2025, the Indian judiciary system interpreted "phishing" in this case, where the plaintiff filed a suit seeking a permanent injunction to prevent the defendants or anyone acting on their behalf from disseminating fraudulent emails that falsely appear to originate from the plaintiff, using the trademark "NASSCOM" or any similar mark in connection with goods or services. Here, the defendant misappropriated the plaintiff's trademark and sent emails to customers, creating the illusion that the correspondence was from NASSCOM. The court ruled that, "Phishing" constitutes a type of internet fraud. In instances of "phishing," an individual impersonates a legitimate entity, such as a bank or insurance company, to obtain personal information from a user, including access codes and passwords, which are then exploited for personal gain, thereby misrepresenting the identity of the legitimate organization.
Generally, "Phishing" scams consist of individuals who impersonate online banking institutions and steal money from e-banking accounts by deceiving consumers into providing sensitive banking information. The various types of Phishing are as follows:

i. Spear Phishing: A focused assault directed at specific individuals or organizations, frequently utilizing personalized data.
ii. Smishing and Vishing: Phishing efforts executed through SMS (smishing) or phone calls (vishing).
iii. Clone Phishing: Cybercriminals produce a nearly exact copy of a genuine email to deceive users.
iv. Pharming: The act of diverting users from a legitimate site to a fraudulent one without their awareness.
v. Email Phishing: Deceptive emails or websites that imitate authentic sources (such as banks or government sites). This is the most prevalent form, where attackers distribute bulk emails that seem to originate from trustworthy entities.

3.0 The Provisions under the Information Technology Act 2000

Phishing is addressed under the Information Technology Act 2000 as follows:

1. Section 43 of the Information Technology Act outlines penalties for unauthorized downloading, damage, etc.: If an individual accesses, downloads, introduces, disrupts, denies, or assists others without the owner's consent, they may be liable for penalties under this section.
2. Section 66 of the Information Technology Act 2000 pertains to computer-related offenses. If a phisher compromises a victim's accounts and engages in any actions specified in Section 43, they may face imprisonment for a term of up to three years, a fine of up to five lakh rupees, or both.

3. Section 66C of the Information Technology Act 2000 addresses identity theft: This provision forbids the use of electronic signatures, passwords, and any unique identifiers of a person. Phishers often impersonate the legitimate account owners to commit fraud.
4. Section 66D of the Information Technology Act 2000 concerns cheating by impersonation: This provision imposes penalties for cheating through impersonation using communication devices or computer resources. Fraudsters create URLs that link to fake websites of banks and organizations, posing as the legitimate bank or financial institution.

4.0 Explanation

All provisions of the Information Technology Act 2000 that pertain to phishing scams are considered bailable offences according to Section 77B of the Information Technology Act 2000 (Amendments 2008). This is due to the ambiguity surrounding the identity of the actual perpetrator. A phisher always operates behind a veil that conceals their identity, which can lead to situations where an innocent individual is wrongfully convicted for a crime they did not commit, resulting in the classification of the offence under this Section as bailable. Additionally, phishing is also classified as an offence under several Sections of the BNS, including Cheating (Section 415), Mischief (Section 425), Forgery (Section 464), and Abetment (Section 107).

5.0 Judicial Response

India's expanding internet user base, projected to exceed 900 million by 2025, creates a prime environment for cybercriminals. Reports of phishing scams have been prevalent in various sectors:

- 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 are taking phishing offenses seriously, particularly when they result in substantial financial losses or data breaches.

In numerous instances, the courts have supported the enforcement of sections from the IT Act 2000 alongside BNS provisions to guarantee stringent penalties in India.

6.0 Cases on Phishing

In the case of NASSCOM v. Ajay Soad & Others, it was recognized as a landmark ruling on phishing. The defendants impersonated NASSCOM (National Association of Software and Service Companies) by sending fraudulent emails to obtain personal data, similar to contemporary phishing attacks. The court determined that phishing is legally defined as "a form of internet fraud" that involves impersonating a legitimate organization to extract personal information. An interim injunction was granted to prevent the misuse of NASSCOM's name, and damages of Rs. 16 lakhs were awarded, emphasizing that intangible harm, such as reputational damage, is eligible for compensation.

In 2018, a man from New York admitted to defrauding a national trade association of over $1.1 million through an email phishing scheme and received the maximum sentence of 20 years in prison.

7.0 Anti Phishing Initiatives

Currently, a range of strategies is being implemented to address phishing, which includes the creation of specific laws and the development of specialized technologies aimed at combating phishing.

- ✓ Strategies for combating phishing through technology.
- ✓ Educating users on recognizing and responding to phishing attempts.
- ✓ Implementation of anti-phishing software: These programs detect phishing content on websites and emails.
- ✓ Utilizing spam filters that also assist in safeguarding users from phishing attacks.
- ✓ Some organizations have adopted distinctive verification methods such as challenge questions and secret images that function as verification passwords.
- ✓ Exercise caution with emails and links. Always verify the sender's email address and be cautious of messages that use urgent language, unfamiliar greetings, or contain spelling mistakes. Refrain from clicking on dubious links or downloading unexpected attachments.

- ✓ Confirm the source; if you receive a message from a bank, company, or government agency requesting personal information, reach out to the organization directly using official contact information.
- ✓ Employ Multi-Factor Authentication (MFA); even if a password is compromised, MFA provides an extra layer of security, making it more difficult for attackers to gain access.
- ✓ Install security software, including antivirus programs, firewalls, and anti-phishing toolbars to identify and prevent phishing threats.
- ✓ Keep systems up to date; ensure that your operating system, browser, and applications are regularly updated with the latest security patches.
- ✓ Monitor your accounts by frequently reviewing bank and credit card statements for any unauthorized transactions.

Additionally, various law enforcement and regulatory agencies are addressing phishing, such as the Indian Cyber Crime Coordination Centre, which issues alerts regarding phishing attacks and cyber threats, Cyber Crime Police Cells, and the National Cyber Crime Reporting Portal, a centralized platform for reporting phishing and other cyber crimes. The RBI Guidelines require two-factor authentication and customer education for banks. The challenges in enforcing measures against phishing in India are as follows.

a) Absence of a Specific Law- India does not have a detailed law addressing phishing.
b) Handling of Digital Evidence- This necessitates trained professionals and forensic tools.
c) International Jurisdictional Challenges- Phishing frequently involves actors from various jurisdictions, complicating investigation and prosecution.
d) Lack of Awareness- Numerous victims fail to identify phishing or are unaware of how to report such incidents.

8.0 The Importance of Public Awareness

- Preventing phishing is not solely reliant on technology; education and awareness play a crucial role. Many effective phishing attacks take advantage of human mistakes instead of software flaws. Thus, increasing awareness can greatly lower the risk of becoming a victim.
- Educational Campaigns: It is essential for governments, educational institutions, and organizations to implement ongoing cyber security awareness initiatives.
- Cyber security in the school curriculum: Incorporating fundamental internet safety and phishing awareness into school programs is vital.
- Simulated Phishing Tests: Companies can perform mock phishing exercises to educate employees on identifying phishing attempts.
- Media Outreach: Leveraging television, radio, social media, and online channels to educate the public about prevalent phishing strategies.

9.0 Best Practices for Individuals

- Refrain from clicking on dubious links or downloading unfamiliar attachments.
- Always verify the sender's email address or phone number.
- Do not share OTPs or passwords, even with individuals claiming to be "officials".
- Utilize strong, unique passwords and activate 2FA (Two Factor Authentication).
- Promptly report phishing attempts to your bank and at https://www.cybercrime.gov.in.

10.0 Conclusion

Combating phishing plays a critical role in enhancing the security landscape of a technologically driven nation like India. Beyond being a mere legal requirement, it stands as a foundational element in building a robust digital ecosystem that safeguards sensitive information and upholds trust in online interactions. Despite the clear importance of addressing phishing activities, it is concerning that India lacks a dedicated legal framework specifically tailored to combat this growWhile the Information Technology Act of 2000 and related regulations offer legal recourse against cybercrimes, including phishing incidents, the absence of a comprehensive statute solely focused on battling this specific challenge poses a notable gap in the current legal landscape. As cybercriminals continually adapt and refine their tactics to perpetrate more sophisticated phishing attacks, relying solely on conventional legal provisions to address these escalating threats proves insufficient in the face of evolving cyber risks. Moving forward, India must consider the imperative of formulating specialized

legislation that precisely targets phishing activities, thereby equipping law enforcement agencies and judicial authorities with the necessary tools to combat this menace effectively. Additionally, raising public awareness about the perils of phishing and educating individuals on identifying and thwarting such deceptive tactics should remain a cornerstone of any overarching strategy to tackle cyber threats comprehensively.

The evolving nature of cyber threats necessitates not only the swift adaptation of legal frameworks to encompass emerging risks but also the active engagement of all stakeholders in promoting a culture of cybersecurity consciousness. By fostering a collaborative environment that integrates legal diligence, technological innovation, and proactive public awareness initiatives, India can effectively fortify its digital defenses against the insidious threat of phishing, ultimately preserving the integrity and trustworthiness of its burgeoning digital landscape.

11.0 References:

1. Prasad & Vandana Rohokale, "Phishing in Cyber Security: The Lifeline of Information and Communication Technology,1 st edition,2020, Springer cham, p33-42.
2. Jyoti Rattan, "Cyber Laws, Information Technology & Artificial Intelligence", 10 th edition, 2023, New Delhi-Bharat Law House Pvt. Ltd. p-657
3. The Information Technology Act 200
4. The BNS
5. The Ministry of Electronics and Information Technology
6. The Supreme court & High Court judgments on cybercrime