INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 6 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 6 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-6-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

LEGAL OBSTACLES IN PHISHING PREVENTION: ADDRESSING JURISDICTION, ACCOUNTABILITY, AND EVOLVING THREATS

AUTHOR - PRANJUL DUBEY* & DR. JYOTI YADAV**

* LLM (CYBER LAW & CYBER SECURITY) AMITY UNIVERSITY, LUCKNOW.

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY, LUCKNOW

BEST CITATION - PRANJUL DUBEY & DR. JYOTI YADAV, LEGAL OBSTACLES IN PHISHING PREVENTION: ADDRESSING JURISDICTION, ACCOUNTABILITY, AND EVOLVING THREATS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (6) OF 2025, PG. 671-678, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

Phishing has become one of the most common and advanced types of cybercrime, impacting both individuals and organizations worldwide. In India, the growing dependence on digital platforms, along with weaknesses in the legal system, creates serious challenges in preventing phishing. This paper looks at the legal difficulties India faces in dealing with phishing, focusing on issues of jurisdiction, accountability, and the constantly changing methods used by cybercriminals. It reviews India's existing laws, such as the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, to assess whether they are effective in tackling phishing. The paper also examines the role of courts and regulatory bodies, offering suggestions for improving laws, strengthening international cooperation, and increasing accountability to better address phishing threats.

Introduction

Phishing is a type of cybercrime where attackers trick people into sharing sensitive information like passwords, credit card details, or personal data. This has become a serious problem in India as the country rapidly adopts digital technologies. With more people using the internet for activities like online shopping, banking, and accessing digital services, phishing attacks have increased. Cybercriminals often take advantage of weaknesses in technology and human mistakes to carry out these scams.

India's growing reliance on digital platforms makes it especially vulnerable to phishing. Attackers create fake websites, emails, or messages that look authentic, convincing people to provide their private information. Despite efforts to improve cybersecurity, the legal system in India has not fully caught up with the challenges posed by phishing. The country's existing laws and policies are not strong enough to handle the sophisticated methods used by cybercriminals.[1107]

One of the main legal challenges is that phishing attacks are often carried out across borders, making it hard to identify and prosecute offenders. These crimes are not limited to one country, and India's law enforcement agencies face difficulties in coordinating with other nations to track down attackers. The lack of clear international agreements or frameworks to deal with cybercrime further complicates the issue.[1108]

Another problem is the unclear accountability of intermediaries, such as internet service

[1107] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[1108] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

providers (ISPs), banks, and social media platforms. These organizations play a key role in detecting and preventing phishing attacks, but current laws in India do not clearly define their responsibilities. For instance, if a phishing attack is conducted through a messaging platform, it's not always clear who is legally responsible—the platform or the attacker.

Moreover, phishing techniques are becoming more advanced with the use of artificial intelligence (AI) and other technologies. Attackers are now able to create convincing fake messages or websites that are difficult to distinguish from real ones. This makes it even harder for individuals and organizations to protect themselves, as traditional cybersecurity measures may not be enough.

To effectively combat phishing in India, several steps are needed. First, the country's laws need to be updated to address the evolving nature of phishing. The Information Technology Act, 2000, and other relevant laws should be revised to include stronger provisions for dealing with cybercrime. Second, there needs to be better collaboration between countries to tackle cross-border phishing attacks. India should actively participate in international efforts to combat cybercrime, such as treaties or agreements for sharing information and resources.

Finally, public awareness and education are crucial. Many phishing attacks succeed because people are unaware of the risks or do not know how to identify scams. Government and private organizations should work together to launch campaigns that teach users how to stay safe online.

Phishing is a growing threat in India that requires a comprehensive approach to prevention. By strengthening its legal framework, improving international cooperation, and raising public awareness, India can better protect its citizens and organizations from this form of cybercrime.

Context -:

Phishing has become a major cybercrime issue in India as the country's digital usage grows rapidly. With more people using online platforms for banking, shopping, and government services, both individuals and organizations are becoming more vulnerable to phishing attacks. These attacks involve cybercriminals tricking people with fake emails, websites, or messages to steal sensitive information like passwords, financial details, or personal data.[3]

Several factors make the problem worse:

- **Increasing Use of Digital Services:** As more people use the internet and digital payments, phishing targets a wide audience, many of whom are not fully aware of cybersecurity risks.
- **Low Awareness:** Many individuals don't understand the risks of phishing or how to protect themselves.
- **Advanced Methods:** Cybercriminals are using new technologies, like AI and social engineering, to make their scams harder to detect.
- **Weak Security :**Measures: Many organizations and individuals lack strong systems to identify and stop phishing attacks.

Although efforts are being made to prevent phishing, challenges remain, especially in terms of improving laws, cooperating with other countries, and educating people to recognize phishing scams. 4

[3] CERT-In, *Annual Report 2022*, Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 6 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

[4] Reserve Bank of India, *Cybersecurity Framework for Banks*, RBI Circular (2021).

Research Questions -:

This paper is guided by the following research questions:

- How do cross-border phishing attacks hinder India's enforcement of cybercrime laws?
- What are the limitations of India's legal framework in addressing international phishing crimes?
- How can India enhance its participation in global cybersecurity initiatives to tackle phishing effectively.

Judicial challenges in Phishing Prevention

Phishing prevention in India faces a major challenge in the form of jurisdiction. Phishing attacks are often carried out by cybercriminals based in foreign countries, making it difficult for Indian law enforcement agencies to take action. India's legal framework, particularly the Information Technology Act, 2000[1109], struggles to address cross-border cybercrimes like phishing because it does not clearly define how to handle crimes that originate outside the country.

One of the main issues arises when phishing attacks are launched from abroad. In such cases, it becomes complex for Indian authorities to take legal action or prosecute offenders. The existing laws in India do not provide sufficient guidelines on how to pursue cybercriminals who operate from other countries. This results in gaps in enforcement, especially when the perpetrators use methods to hide their location or identity, such as using Virtual Private Networks (VPNs) or fake IP addresses.

An important international framework to help with such challenges is the Budapest Convention[1110] on Cybercrime, which aims to standardize cybercrime laws across countries and improve international cooperation. The convention facilitates the sharing of information between nations to combat cybercrimes, including phishing, and ensures that offenders are held accountable no matter where they are located. However, India is not a signatory to the Budapest Convention, which limits its ability to cooperate with other countries when dealing with international cybercrimes. The lack of such international cooperation makes it harder for India to trace the origins of phishing attacks and prosecute perpetrators effectively.

In addition to not participating in international frameworks like the Budapest Convention, Indian laws also lack clear provisions for cross-border cybercrime cooperation. This means that even if a phishing attack originates outside India, it is challenging for Indian authorities to request information or legal assistance from foreign governments or organizations.

The absence of such provisions further weakens India's ability to address phishing crimes that occur beyond its borders.

The frequency of phishing attacks originating from outside India has been increasing, making the need for stronger international cooperation even more urgent. Phishing attacks can now be launched from anywhere in the world, and without effective international collaboration, criminals can exploit differences in laws across countries. For example, cybercriminals may target victims in India while operating from regions with weaker laws or less strict enforcement, making it difficult to bring them to justice.

To address these challenges, India needs to improve its approach to jurisdiction in the context of cybercrimes. A key step is to strengthen its participation in international treaties like the

[1109] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 75 (India).

[1110] Budapest Convention on Cybercrime, Council of Europe, ETS No. 185 (2001).

Budapest Convention to foster better cooperation with other countries. This would allow India to share information, request legal assistance, and take collective action against phishing and other forms of cybercrime more effectively.

Additionally, Indian laws should be updated to provide clear guidelines on handling cross-border cybercrimes. This could include creating specific provisions for cybercrime cooperation, making it easier for law enforcement agencies to act against phishing attacks that cross international borders.[1111] Without these legal improvements, India will continue to face significant challenges in combating phishing, especially as attackers become more sophisticated and operate across multiple jurisdictions.

Jurisdictional challenges are a critical obstacle in phishing prevention in India. Strengthening international collaboration and updating domestic laws to address cross-border crimes are essential steps toward improving the country's ability to combat phishing attacks.

Accountability and Liability of Intermediaries

In India, one of the key obstacles in preventing and addressing phishing is the issue of accountability, particularly concerning intermediaries. Under Section 79 of the Information Technology Act, 2000,[1112] intermediaries such as Internet Service Providers (ISPs), social media platforms, and email hosts are granted safe harbor provisions. This means that intermediaries are not held liable for the content they host or transmit unless they are directly involved in the commission of a cybercrime.

However, this provision creates a grey area in phishing cases. Intermediaries often play a significant role in enabling phishing attacks, either by hosting fraudulent websites or failing to detect phishing emails. The lack of clarity regarding their proactive responsibility to monitor and prevent phishing activities undermines effective enforcement and victim protection.

The Digital Personal Data Protection Act, 2023, which addresses data security, does not specifically tackle intermediary liability in the context of phishing. While the law mandates data controllers to take steps to secure personal data[1113], it does not explicitly require intermediaries to prevent or mitigate phishing attacks. This regulatory gap needs to be addressed by revising the legal framework to ensure that intermediaries have a duty to actively monitor and report phishing activities and are held accountable for their failures.

Evolving Phishing Techniques and Legal Adequacy

Phishing attacks have become significantly more advanced, with cybercriminals adopting increasingly sophisticated techniques. Modern phishing tactics, including spear-phishing, AI-generated deepfakes, and various social engineering methods, are more difficult to detect and prevent. These new strategies often bypass traditional security defenses and manipulate human psychology, making them more effective. However, India's current legal framework, primarily shaped by the Information Technology Act, 2000, was designed at a time when phishing was a simpler form of cybercrime. As a result, the Act struggles to adequately address the evolving and complex nature of phishing attacks today.[1114]

The Information Technology Act, 2000 was drafted before the rise of more advanced phishing techniques, and it mainly focuses on basic forms of cybercrime and online fraud. While it has been updated over time, the

[1111] Praveen Dalal, *International Cybersecurity Cooperation: Challenges for India*, 45 *J. Cyber L.* 82 (2020).

[1112] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 79 (India).

[1113] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 9 (India).

[1114] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

legislation still does not fully cover the intricacies of modern phishing, especially the more targeted approaches like spear-phishing or those that use deepfake technology. These sophisticated tactics often go undetected by traditional security measures and exploit psychological vulnerabilities, such as creating a sense of urgency or trust, which makes them especially dangerous.[1115]

In response to growing concerns about data privacy and security, India introduced the Digital Personal Data Protection Act (DPDP Act), 2023, aimed at enhancing personal data security and privacy protections. While the DPDP Act represents an important step forward, particularly regarding how personal data is handled by organizations, it still does not fully address the unique challenges posed by modern phishing tactics. The Act does not specifically account for phishing techniques that leverage social engineering, AI-powered tools, or the exploitation of human behavior. Therefore, although the DPDP Act is a step in the right direction, it does not provide a comprehensive solution for combating advanced phishing threats.[1116]

The gap between the rapid advancement of phishing methods and the slow pace at which legal frameworks evolve leaves individuals and organizations in India vulnerable to increasingly complex cyberattacks. Phishing attacks, especially those that use sophisticated technology, are growing in scale and impact, posing significant risks to privacy, financial security, and the trustworthiness of digital platforms.

For India's legal system to effectively combat modern phishing threats, it is crucial that the legal framework be updated to specifically address new phishing tactics. Laws must evolve to stay in line with the changing landscape of cybercrime and technological advancements. Additionally, judicial bodies and law enforcement agencies must be equipped with the tools and expertise needed to tackle the technical complexities of modern phishing attacks. This includes training for law enforcement on identifying and responding to advanced phishing tactics and ensuring that there are clear procedures in place to investigate and prosecute such crimes.

Phishing techniques continue to evolve, India's legal framework must adapt to effectively address these emerging threats. Laws must be updated, and law enforcement agencies must be empowered with the necessary knowledge and tools to deal with the increasingly sophisticated nature of phishing attacks. Without these adaptations, India will struggle to protect its citizens and organizations from the growing threat of phishing.

Awareness, Reporting, and Victim Protection

One of the key obstacles in preventing phishing attacks in India is the widespread issue of underreporting. Many victims of phishing attacks choose not to report the incidents due to various reasons, including a lack of awareness about the potential consequences of such attacks, fear of damage to their reputation, or the belief that reporting the crime will not lead to any substantial results. This reluctance to report phishing attacks significantly hinders the ability of law enforcement agencies to track phishing trends, investigate the scale of the issue, and develop appropriate responses. Without comprehensive data on the frequency and types of phishing incidents, authorities struggle to understand the full scope of the problem and to design effective prevention strategies.[1117]

In addition to underreporting, the current system lacks adequate victim protection mechanisms. Phishing attacks often lead to

[1115] Ministry of Electronics and Information Technology, *National Cyber Security Policy 2023*, Government of India.

[1116] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

[1117] Reserve Bank of India, *Fraud Monitoring Guidelines*, RBI Circular No. DBOD.BP.BC.116/2022-23.

financial losses for individuals and organizations, but there are few legal provisions that clearly define how victims should be supported or compensated. While the Information Technology Act, 2000 and other regulations address cybercrimes, they do not specifically cover compensation for victims of phishing attacks. This lack of victim-centric provisions leaves many individuals without the necessary legal recourse to recover their losses. Furthermore, financial institutions, digital platforms, and other intermediaries involved in the transaction processes often do not bear the responsibility for lapses in their security systems, further exacerbating the problem.[1118]

The absence of clear guidelines and obligations for financial institutions, social media platforms, and other online service providers complicates the situation, as there is no accountability for their role in facilitating phishing attacks through weak security practices or lack of monitoring. While financial institutions are expected to maintain robust security protocols to protect their users, many phishing victims find it difficult to secure compensation or even basic support after falling victim to fraud. Similarly, digital platforms and service providers may not always be held liable for phishing activities that occur through their networks, despite their role in enabling these attacks.

To tackle these challenges, it is essential to create a more effective and user-friendly reporting system that encourages victims to come forward without fear of repercussions. A major component of this system should include public awareness campaigns aimed at educating both individuals and organizations about the risks of phishing, how to recognize phishing attempts, and how to report such incidents effectively. Many victims are not aware that they can report phishing to authorities or their service providers, leading to a missed opportunity for early detection and mitigation of phishing schemes.

Along with improving the reporting infrastructure, it is also critical to develop legal provisions that ensure victims of phishing attacks receive adequate support. This includes introducing measures to hold financial institutions and digital platforms accountable for lapses in their security measures. If a platform or institution fails to take necessary precautions to safeguard their users from phishing attacks, they should be legally obligated to compensate the victims for their financial losses. These steps would go a long way in protecting citizens from the financial and emotional distress that often follows a phishing attack. Furthermore, creating a more transparent process for victim compensation would make it easier for individuals to seek redress and restore their confidence in the digital economy.

Recommendations

Based on an in-depth analysis of India's existing legal framework and the challenges posed by phishing, several recommendations can be made to strengthen phishing prevention and victim protection in the country. These recommendations aim to address jurisdictional issues, improve the legal framework to adapt to evolving phishing techniques, enhance victim support mechanisms, and promote international cooperation in the fight against cybercrime.

- **Jurisdictional Reforms:** One of the most pressing issues in addressing phishing attacks in India is the difficulty of dealing with cross-border cybercrimes. As phishing attacks often originate from outside India, it is essential for India to actively pursue participation in international

  frameworks such as the Budapest Convention on Cybercrime. This international treaty is designed to standardize laws related to cybercrime

[1118] Indian Computer Emergency Response Team (CERT-In), *Phishing and Reporting Framework*, Ministry of Electronics and Information Technology, Government of India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 6 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and improve cooperation among nations in investigating and prosecuting cybercriminals. By becoming a party to the Budapest Convention, India would strengthen its ability to collaborate with other countries in addressing phishing and other forms of cybercrime.[1119]

Additionally, India should establish clearer jurisdictional guidelines to ensure that law enforcement agencies can pursue and prosecute cybercriminals across borders more effectively.

- **Revising Intermediary Liability:** Another key area that requires attention is intermediary liability. Section 79 of the Information

Technology Act, 2000, provides a safe harbor to intermediaries such as internet service providers (ISPs), social media platforms, and email hosts, shielding them from liability for user-generated content.[1120]

However, this provision does not impose a proactive responsibility on these intermediaries to prevent or detect phishing activities occurring through their platforms. To address this gap, India should amend Section 79 to make intermediaries more accountable. This could involve requiring intermediaries to implement stronger security protocols, monitor for phishing attempts, and cooperate with law enforcement agencies in identifying and addressing phishing attacks.

By holding intermediaries accountable for the security of their platforms, the risk of phishing attacks can be significantly reduced

- **Adapting to Evolving Threats:** As phishing techniques continue to evolve, with attackers using AI-powered tools and sophisticated social engineering tactics, India's legal framework must adapt accordingly. The Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, represent important steps toward regulating cybersecurity and data privacy, but they still fall short in addressing the complexities of modern phishing techniques. For instance, AI-driven phishing attacks, such as those using deepfake technology to

impersonate individuals or organizations, are not adequately covered by existing laws. To stay ahead of these threats, India must update its legal framework to include provisions that specifically target new and emerging phishing techniques. These updates should ensure that law enforcement and judiciary agencies are well-equipped to handle the challenges posed by sophisticated cybercrimes.[1121]

- **Enhancing Victim Support and Reporting:** To encourage reporting and ensure that victims are properly supported, India needs to introduce clearer mechanisms for reporting phishing incidents and offering compensation. This could involve creating dedicated online portals where victims can easily report phishing attacks and track the progress of investigations. Public awareness campaigns should be launched to educate individuals and businesses about how to recognize phishing attempts, report them to the relevant authorities, and seek redress.

Additionally, financial institutions and digital platforms must be held accountable for lapses in security, and victims of phishing attacks

[1119] Budapest Convention on Cybercrime, Council of Europe, ETS No. 185 (2001).

[1120] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 79 (India).

[1121] Ministry of External Affairs, *India's Cyber Diplomacy: Towards Global Cooperation*, Government of India (2023).

should be entitled to compensation for financial losses caused by these incidents. These measures would provide stronger protection for victims and reduce the fear of reporting.

- **Fostering International Cooperation**: Given that phishing attacks often involve cross-border elements, India must strengthen its international cooperation to combat cybercrime. Bilateral and multilateral agreements should be established to improve coordination between Indian authorities and their counterparts in other countries.

This could include sharing information about phishing trends, conducting joint investigations, and supporting the prosecution of

cybercriminals who operate internationally. International collaboration will enhance India's capacity to prevent and respond to phishing attacks, ultimately making it more effective in addressing cybercrime.

Conclusion

Phishing continues to pose a significant threat to individuals and organizations in India, with challenges arising from jurisdictional issues, evolving attack techniques, underreporting, and a lack of victim support mechanisms. Addressing these challenges requires comprehensive legal reforms and greater international cooperation. By participating in international frameworks, revising intermediary liability laws, adapting to new phishing threats, improving victim support systems, and enhancing public awareness, India can create a more robust system to prevent and respond to phishing attacks. A multi-pronged approach, combining legislative updates, stronger law enforcement, and better victim protection, will be essential in safeguarding citizens and organizations from the increasing risks posed by phishing in the digital age.[1122]

References-:

- Information Technology Act, 2000, Government of India.
- Digital Personal Data Protection Act, 2023, Government of India.
- The Budapest Convention on Cybercrime.
- United Nations Office on Drugs and Crime (UNODC), "Cybercrime and the Role of

International Cooperation," 2020.

- India Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of india.

[1122] Ministry of Home Affairs, *India Cyber Crime Coordination Centre (I4C)*, Government of India.