

PHISHING ATTACKS IN INDIA: AN ANALYSIS OF EMERGING TECHNIQUES, DETECTION STRATEGIES AND 2025 FRAUD TRENDS

Dr. Navpreet Kaur
Pt. C.L.S. Government College, Karnal

Abstract Phishing is a deceptive cybercrime in which attackers impersonate as an authentic organizations, person or services to gain any individual's trust and obtain their private information such as financial credentials, login details, net banking accounts and other useful information. This cybercrime has moved beyond conventional fraudulent emails and now operates across SMS, voice calls, social-media platforms, fake websites, QR codes and other digital communications. I reviewed earlier studies on phishing attacks and detection, synthesizes their main findings, and places them against the Indian cyber-fraud environment reported by government agencies in 2024-25. The review shows a clear progression from rule-based and blacklist-oriented protection towards machine-learning, natural-language processing, pattern analysis and hybrid detection. Random Forest and Support Vector Machine approaches repeatedly show strong performance in the reviewed literature, while NLP-based analysis is useful for extracting linguistic indicators from messages. As phishing data and attacker approach change over time so highly precise data is also vulnerable. Indian government records underline the scale of the wider cyber-fraud problem: the Ministry of Home Affairs reported 3,822,550 cyber-fraud incidents through the National Cyber Crime Reporting Portal from inception to January 2025, with ₹ 3,644,819.85 lakh reported as the amount involved. In a separate 2025 government reply reported that the Citizen Financial Cyber Fraud Reporting and Management System had helped save more than ₹ 5,489 crore across more than 17.82 lakh complaints. CERT-In also reported a major national cyber-incident workload for 2024-25. The paper argues for a layered model combining sender authentication, URL and content analysis, machine learning, signals, threat intelligence, user awareness and rapid reporting. Rather than treating phishing as only a technical classification problem, the study presents it as a socio-technical problem in which technology and human judgement must work together to achieve so concrete solution. **Keywords:** Phishing; cyber fraud; social engineering; smishing; vishing; machine learning; NLP; Random Forest.

1. Introduction

The service like online and digital have become integral part of everyday life, including banking, shopping, education, professional communication and public services etc. This has given the number of opportunities available to attackers who rely on deception rather than on direct compromise of technical infrastructure. Phishing is especially effective because the attacker often needs only to persuade a person to perform one action: open a link, download a file, disclose a credential, approve an authentication request or transfer money to some external request. The literature consistently describes phishing as an impersonation-based form of social engineering in which the attacker attempts to make a malicious communication appear trustworthy and legitimate. The nature of phishing has nevertheless changed. Earlier examples were poorly written emails and visibly suspicious URLs. Contemporary campaigns can use convincing branding, personalized information, shortened or deceptive links, fake

login pages, social-media messages and voice communication. The 2024 study also notes the growing use of generative AI to make phishing content more convincing, while the 2025 survey identifies real-time analysis, behavioural modelling and hybrid systems as important directions. This paper compares the principal detection approaches—signature/list based, heuristic, NLP, machine learning, behavioural and hybrid detection. And Indian perspective using government records and advisories from 2024-25.

2. Various phishing methods of cyber attacks

Phishing is a cluster of techniques rather than a single attack. One of the primarily used method is Email phishing. Spear phishing is directed at a particular person or organization and normally uses information gathered about the target to make the message plausible. Smishing moves the same social-engineering idea to SMS or messaging services. Vishing uses phone calls and can exploit authority, fear or urgency. Website phishing relies on fraudulent pages that imitate legitimate services. Search-engine or advertisement-based phishing can place deceptive results where a user expects a genuine service. The reviewed literature also discusses covert redirection, in which apparently legitimate links or authentication flows can be abused to move a victim towards attacker-controlled infrastructure. A major change is the role of personalization. Publicly available information can be used to construct a message that refers to a person's employer, role, recent activity or expected transaction. This reduces the usefulness of simple spelling-based detection. It can be from credential theft towards session and identity abuse. Modern authentication systems can be targeted through fake sign-in pages, malicious authentication requests or attempts to capture tokens and sessions.

3. The identification and Prevention Approaches

Signature and blacklist methods are fast and relatively easy to deploy. They are effective when an attack indicator is already known, but they are inherently reactive: a newly created malicious domain may not yet appear in the database. The 2024-25 survey therefore treats list-based detection as one component rather than a complete solution. In Heuristic detection the idea is to examining suspicious properties such as misspelled domains, unusual URL structure, excessive redirects, urgency, unreliable attachments. Heuristics can detect patterns that have not yet been assigned a specific signature, but they can also generate false positives when legitimate messages resemble known attack patterns. In NLP-based detection treats the message itself act as data. Pre-processing can include tokenization, stopword removal, case normalization, stemming and keyword extraction at the receiver's end. Features can then be combined with sender, URL and header information. The NLP/Random Forest study demonstrates a practical architecture in which suspicious messages are analyzed and then classified. [In machine learning we can use a set of various rules instead of relying on single one. The 2024-25 survey reports strong results for Random Forest and SVM across the reviewed literature, with several reported datasets producing accuracy values above 90%. However, these values are dataset-dependent. A model trained on older phishing messages can perform less reliably when attackers change vocabulary, domains, page layouts or delivery channels and its limitations. Behaviour-based detection technique includes analyzing deviations from normal things, such as unusual interaction patterns or anomalous browsing behaviour. Its advantage is the ability to identify activity that has not been seen before; its

limitations include privacy, baseline quality and the difficulty of separating unusual legitimate behaviour from malicious activity. The strongest direction emerging from the reviewed papers is therefore hybrid detection. A practical architecture can combine sender authentication and reputation checks, URL and content heuristics, an ML classifier.

4. Indian perspective of Cyber-Frauds in 2025

In Indian context phishing should be taken alongside the wider cyber-fraud ecosystem as equally important. In a Rajya Sabha answer dated 12 March 2025, the Ministry of Home Affairs reported 3,822,550 cyber-fraud incidents on the National Cyber Crime Reporting Portal from inception to January 2025. The amount reported was ₹ 3,644,819.85 lakh, while ₹ 438,080.57 lakh was placed under lien and ₹ 6,051.65 lakh was shown as refunded. These figures cover cyber-fraud complaints broadly and should not be interpreted as phishing-only counts. The government answer describes the Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System. It also states that CERT-In works with service providers, regulators and law-enforcement agencies to track and disable phishing websites. The answer records more than 8 lakh suspect records and more than 20 lakh mule accounts shared through the suspect registry at that point, with more than ₹ 2,889 crore saved. In a Lok Sabha reply provides another indication of the operational response. The government reported that the Citizen Financial Cyber Fraud Reporting and Management System had saved more than ₹ 5,489 crore across more than 17.82 lakh complaints. It also reported the blocking of more than 9.42 lakh SIM cards and 2,63,348 IMEIs based on police inputs, and the sharing of more than 11 lakh suspect identifiers and 24 lakh Layer-1 mule accounts. These measures illustrate that modern anti-fraud work extends beyond identifying a phishing message and it also involves telecom controls, financial institutions, law enforcement, intelligence sharing and rapid intervention thereafter. Government reporting also shows the scale of the broader national cyber-security workload. A Ministry of Home Affairs/PIB release in 2024-25, reporting CERT-In's 2025 figures, states that 29,44,248 cyber-security incidents were observed in 2024-25. This is a broad cyber-incident count rather than a phishing count, but it provides useful context for the volume of activity that national response systems must handle. In CERT-In's 2024-25 advisories further emphasized security hygiene, including multi-factor authentication, employee awareness, monitoring, incident response and zero-trust principles. Its May 2025 advisory specifically recommended regular cybersecurity training and phishing simulation exercises for organizations and institutions.

5. Some of the phishing Attack Patterns and Government Response

The available government evidence does not provide a single official table of 'phishing attacks in India during 2024-25 separated by phishing subtype. The government records of 2024-25 were used to see threat environment and the mechanisms deployed against fraud and phishing-related infrastructure details. One important pattern is impersonation-based fraud. Government awareness programs in 2024-25 specifically addressed digital-arrest scams and other social-engineering methods through SMS, television, radio, school campaigns, public transport messaging and other means. The industrialization of fraud infrastructure is another aspect. The I4C model described by the government links banks,

payment intermediaries, telecom operators, IT intermediaries and State/UT law-enforcement agencies through the Cyber Fraud Mitigation Centre. Such coordination is particularly important when an attacker uses a phishing message to initiate a financial transfer, because stopping the loss may require action after the initial message has already reached the victim. Next measure is increasing importance of infrastructure-level controls. The government reported mechanisms for identifying and blocking spoofed international calls that display Indian numbers, while CERTIn continues to issue alerts and advisories and coordinate with providers to disable malicious data and communications. These measures complement message-level detection and show why phishing prevention must operate at several points in the attack chain. So, a layered interpretation of phishing defence is required which includes; detect suspicious content, verify identities and domains, warn the user, monitor subsequent activity, provide fast financial reporting, and coordinate with telecom, banking and law-enforcement systems. The effectiveness of the overall system depends on how quickly these layers exchange information and respond in time.

Phishing Indicator of 2025:

A government-reported indicator provides a more specific measure of phishing activity than the broader cyberfraud totals discussed above. Prior to the spike identified by the National Critical Information Infrastructure Protection Centre (NCIIPC) during early 2025, coordinated actions between the Ministry of Home Affairs' Indian Cybercrime Coordination Centre (I4C) and domain partners proactively identified and disabled malicious platforms. During the full year of Jan–Dec 2024, official metrics captured 580 phishing domains specifically targeted and neutralized under primary internet exchange collaborations. A sharp uptick was observed immediately moving into January 2025, which recorded 195 malicious domains in that single month alone as threats against Critical Information Infrastructures scaled up. This figure is useful as a commercial/critical-infrastructure phishing indicator but should not be interpreted as the total number of general phishing attacks across all Indian commercial businesses.

Figure Y. Phishing domains targeting India's Critical Information Infrastructure — 2024 to Jan 2025

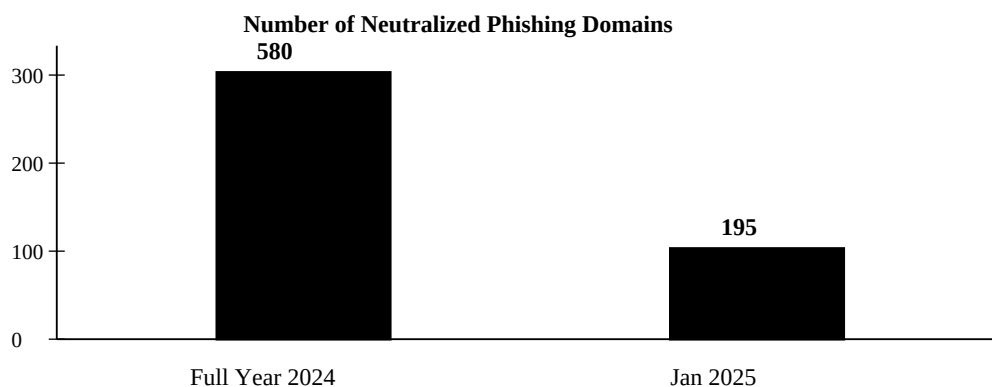


Figure Y. Phishing domains targeting India's Critical Information Infrastructure — 2024 to Jan 2025

Number of Neutralized Phishing Domains

6. Comparative Analysis of different methods

The various approaches can be compared on four bases: uncovering of known attacks, ability to recognize new attacks, computational/operational cost, and dependence on data or user behavior. Some of the important findings are; Blacklist and signature systems score well on speed and simplicity but poorly on novel attacks. Heuristics are more flexible but can create false positives. NLP and supervised ML can capture combinations of linguistic and technical indicators, but they depend on representative training data. Behavioural analysis can detect previously unseen activity, yet it raises privacy and baseline-quality questions. Hybrid systems require greater engineering effort but can distribute the weaknesses of one method across several layers. The literature also shows why benchmark accuracy should be interpreted carefully. A Random Forest model may report very high accuracy on a static dataset while encountering difficulty with new domains or message styles in production. Conversely, a simple rule may have lower benchmark accuracy but remain valuable because it is transparent, inexpensive and immediately useful for known threats. For India, another criterion is response time. The I4C financial-fraud system is designed around immediate reporting because money can move rapidly through accounts. This means that prevention and recovery cannot be separated cleanly. A detection system that flags a suspicious message but provides no clear reporting or intervention path is incomplete from a real-world perspective and it needs improvement.

7. Solution oriented Layered Framework

A phishing defence framework can be Have six layers to be more solution oriented. Layer 1 performs identity and sender checks, including SPF, DKIM and DMARC where applicable. Layer 2 examines URLs, domains, redirects, attachments and page characteristics. Layer 3 analyses message language with NLP features such as use of urgent word, impersonation cues and unusual texts. Layer 4 applies a machine-learning classifier such as Random Forest or another suitable ensemble model. Layer 5 monitors behavioural and contextual signals, including suspicious browsing activity or login requests.

The sixth Layer will have decision engine to current threat intelligence, user warnings, incident reporting and will respond accordingly. The key improvement over a single classifier is feedback. Newly confirmed phishing messages, malicious domains and user reports should be fed back into detection systems after suitable validation. This reduces the delay between the appearance of a new campaign and the creation of a usable detection signal. The process should also preserve analyst review for uncertain cases, since excessive automation can produce false positives and unnecessary blocking. For educational institutions and small organizations, the same model can be simplified. Email filtering and sender authentication can form the first line, followed by browser protection and basic URL check. Training at regular intervals should be there for staff and students. Simulated phishing exercises can be used to measure improvement, provided that they are conducted ethically and do not collect unnecessary personal information of the persons. CERT-In's 2024 guidance supports regular awareness and phishing-simulation exercises. For financial and public-service environments, the framework should additionally support rapid escalation. A suspicious message that requests a payment should trigger an independent verification step, and suspected financial fraud should be reported immediately through the official channels. The channels to tackle these are like 1930 helpline and National Cyber Crime Reporting Portal.

8. Conclusion and Future Scope

The central finding of this review is that phishing is no longer adequately represented by the traditional picture of a suspicious email containing a bad link. The attack surface now includes multiple channels, and the most effective campaigns exploit context as much as technical weaknesses. This changes the design requirement for detection systems: they must combine message-level evidence with identity, URL, behavioural and threatintelligence signals. The second finding is that machine learning should be treated as an adaptive component rather than a final answer. The 2024-25 survey shows strong results for RF and SVM, but also identifies generalisation and scalability as continuing problems. A model's usefulness therefore depends on how frequently its data are refreshed, how representative the evaluation set is, and whether it is tested against genuinely new problems or not. The third finding concerns the human role. Social engineering works because users make decisions under time pressure, uncertainty or perceived authority. Technical controls can reduce exposure, but they cannot eliminate every situation in which a legitimate-looking request is presented through a trusted channel. Clear warnings, independent verification habits and rapid reporting remain essential and it should include timely trainings. Finally, the Indian government response indicates that phishing and cyber fraud cannot be handled by one organization. CERT-In, I4C, banks, telecom operators, intermediaries and State/UT law-enforcement agencies each occupy a different role in strategy. So, a strict policy is needed to tackle this. Future work should also investigate explainable hybrid models, privacy-preserving behavioural analysis, multilingual NLP for Indian languages, real-time threat-intelligence integration and evaluation against AI-assisted social engineering. Such work can help shift phishing defence from reactive blocking towards continuous, context-aware risk management and policies

References

- [1] R. Tanti, “Study of Phishing Attack and their Prevention Techniques,” International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 8, no. 10, Oct. 2024, DOI: 10.55041/IJSREM38042.
- [2] B. Bajanthri and S. Sayeesh, “A Study on Various Phishing Techniques and Recent Phishing Attacks,” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 2, no. 2, Mar. 2022, DOI: 10.48175/IJARSCT-2870.
- [3] A. Anand and S. K. M. Sowmyashree, “Email Phishing Detection in Cybersecurity,” International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 8, Aug. 2021, ISSN 2320-2882.
- [4] S.K Gupta and N. Sharma, “A comprehensive review of machine learning and deep learning approaches for phishing website detection Survey and comparative analysis of phishing detection,” Journal of Cyber Security Technologies , vol. 08, no. 1, pp. 45-68, January 2024
- [5] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 258, “Grievance Redressal and Advisories against Online/Cyber Frauds,” answered 27 November 2024.
- [6] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 1579, “Advertisement of online frauds and Cyber security measures ,” answered 04 December 2024..
- [7] Government of India, Ministry of Home Affairs/National Crime Records Bureau(NCRB), “Crime in India 2023 Report: Focus on Rising trends in digital offenses and cyber crimes,” published in December 2024.
- [8] R. Kumar and A. Mathew, “Evolving paradigm in Cyber crime: A survey of phishing detection mechanism, challenges and future horizons,” International Journal of Information Security, vol 23, no.3 pp 11021120, May 2024.
- [9] Indian Computer Emergency Response Team (CERT-In), “Cyber Security Handbook,” 2024.
- [10] CSIRT-Fin, CERT-In, and Mastercard, “API Security: Threats, Best Practices, Challenges, and Way forward using AI,” Ministry of Electronics and Information Technology, Government of India, 2023. Available: <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADV01&CACODE;=CICA-2023-3248>.
- [11] Indian Computer Emergency Response Team (CERT-In), “ Measures to Prevent IDOR Vulnerabilities,” Advisory CIAD-2024-0051, 01 November 2024. Available: <https://www.cert-in.org.in/s2cMainServlet?Pageid=PUBVLNOTES02& VL CODE=CIAD- 2024-0051>.

- [12] Indian Computer Emergency Response Team (CERT-In), “Cyber Security Awareness Booklet,” Government of India. Available: https://www.cert-in.org.in/PDF/CSA_Booklet.pdf.
- [13] Reserve Bank of India (RBI), “Annual Report 2023-24,” Chapter on Consumer Review, Protection and Ombudsman Scheme, 2024. Available: <https://www.rbi.org.in>
- [14] Reserve Bank of India (RBI), “Monetary and Credit Information Review,” Vol. XIX, Issue 10, January 2024
- [15] National Payments Corporation of India (NPCI), “Fraud Awareness,” official consumer awareness resource. Available: <https://www.npci.org.in/fraud-awareness>.
- [16] National Payments Corporation of India (NPCI), “Abridged Minutes of UPI and Services Steering Committee Meeting, 24 January 2025,” 2025. Available: <https://www.npci.org.in/PDF/npci/upi/steeringcommittee/2025/Abridged-Minutes-of-UPI-Steering-Committee-Meeting-held-on-24th-January-2025.pdf>.
- [17] Indian Computer Emergency Response Team (CERT-In), “Preventing Online scams,” Advisory CIAD-20250050, October 2024