Managing DNS Abuse: Perspective from .IN Registry

Presented by: Dr. Devesh Tyagi

DNS Abuse Mitigation activities

1. Domain Name keyword verification

2. WHOIS verification

3. Incorporation with Indian LEAs

Empowering Netizens

Checking of identification for Foreign Nationals

- As part of the verification process, .IN Registry verify registrant details using documents such as a passport, citizenship ID, and other accepted relevant identification.

- Further, under the **new RAA Clause 4.4.15**, foreign applicants requesting a .IN domain must also demonstrate a legitimate business connection or purpose in India.

Abuse Mitigation

Initiative since Oct’23 for Monitoring Domain Registration

NIXI has initiated enhanced monitoring of domain registrations through the following measures:

- Placing well-known and sensitive keywords such as gov, nic, bharat, etc., on a reserved list to prevent misuse.
- Since May 2024, implementing a real-time mechanism to flag and block domain registrations made by repeat offenders using abusive email IDs or mobile numbers.
- Conducting manual verification of domain name WHOIS details.
- Reviewing and acting upon domain name lists received from agencies such as CERT-In, Indian Cyber Crime Coordination Centre (I4C), and other LEAs.

Regular Monitoring of Domain Registration Since Oct, 2023

- NIXI has established a regular monitoring mechanism under which domains registered on a daily basis are systematically scrutinized. This initiative aims to detect and prevent cybercrime, phishing activities, and potential reputational damage.
- A keyword list has been developed based on inputs from LEAs, MeitY, and NIXI. The list includes sensitive terms such as PMO, Reserve Bank of India (RBI), banks, Central Bureau of Investigation (CBI), Government schemes, Supreme Court of India, courts, and other related keywords.
- Through continuous monitoring of domain registrations and flagging domains containing such sensitive keywords, NIXI proactively identifies and mitigates potential threats by reporting them to the concerned institutions and the Indian Cyber Crime Coordination Centre (I4C).
- Potential threats involving RBI- and CBI-related keyword domains have been successfully mitigated and notified through this proactive monitoring framework.

Implemented mechanism since May’24 to flag and block domains booked in real-time - abusive email Address and mobile number

Domain Found In Banned List

Domain	ROID	Registrar	Banned Contact	Activity From	Activity To	Cron End Time
supremejudicialauthority.in	DE940DFBAAB2E4666AA0040BDEF0439B7-IN	Dynadot LLC	Yes :- deaksafrancke414@gmail.com ### +66.620391761	2024-12-11 11:15:01	2024-12-11 11:30:01	2024-12-11 16:15:09

Statistics of Malicious activities

Threat Report - Statistics

- Law Enforcement Agency
- Indian Cybercrime Coordination Centre (I4C)
- CERT-In
- Manual checking of KYC and eKYC

Threat Report Statistics – Law Enforcement Agency

Month	2023	2024	2025	2026
Jan		1	0	1
Feb		10	1	
Mar		14	4	
Apr		9	0	
May		25	0	
Jun		0	0	
Jul		3	11	
Aug		2	3	
Sep		3	0	
Oct	40	2	0	
Nov	45	3	3	
Dec	9	6	1	
Total	**94**	**78**	**23**	**1**

Threat Report Statistics – Indian Cybercrime Coordination Centre (I4C)

Month	2023	2024	2025	2026
Jan		41	0	0
Feb		21	1	
Mar		45	1	
Apr		48	4	
May		24	3	
Jun		5	0	
Jul		7	4	
Aug		1	0	
Sep		6	1	
Oct	34	8	0	
Nov	54	4	3	
Dec	43	1	0	
Total	**131**	**211**	**17**	**0**

Threat Report – Received from CERT-In

Month	2023	2024	2025	2026
Jan		46	11	7
Feb		94	12	
Mar		75	50	
Apr		37	26	
May		62	25	
Jun		0	2	
Jul		38	22	
Aug		37	13	
Sep		43	5	
Oct	16	50	3	
Nov	10	14	7	
Dec	15	10	1	
Total	**41**	**506**	**177**	**7**

Note: Typo-Squatting domain like **bajajfinanc.in, creditardapply.co.in, slcn.in etc.**

Threat Report – Manual KYC and eKYC

Month	2023		2024		2025		2026	
	Put on Hold	Released	Put on Hold	Released	Put on Hold	Released	Put on Hold	Released
Jan			2,766	328	6,323	723	4,186	644
Feb			2,716	497	4,237	843		
Mar			2,882	486	5,364	1,320		
Apr			3,126	648	5,890	768		
May			2,981	530	8,624	424		
Jun			2,430	480	1,276	467		
Jul			2,730	426	6,069	866		
Aug			2,733	462	20,296	1,148		
Sep			7,971	1,063	17,912	1,683		
Oct			6,680	1,311	3,886	890		
Nov			5,563	1,148	3,173	776		
Dec	830	67	8,096	557	3,724	700		
Total	**830**	**67**	**50,674**	**7,936**	**86,774**	**10,608**	**4,186**	**644**

*As per the latest SURBL report, .in appears to be at serial number 58 with 2,276 count.

S.No.	TLD	Count
58	in	2276

Initiative to Prevent Domain Abuse

- Directed all registrars, including international registrars, to implement mandatory KYC requirements.

- Collaborated with Law Enforcement Agencies (LEAs) during major international events and sensitive occasions such as G20, Ayodhya, and Operation Sindoor to ensure cybersecurity preparedness.

- Developed Standard Operating Procedures (SOPs) and best practices for the .IN Registry and submitted them to I4C (MHA).

New Registrar Accreditation Agreement (RAA) to make .IN more secure

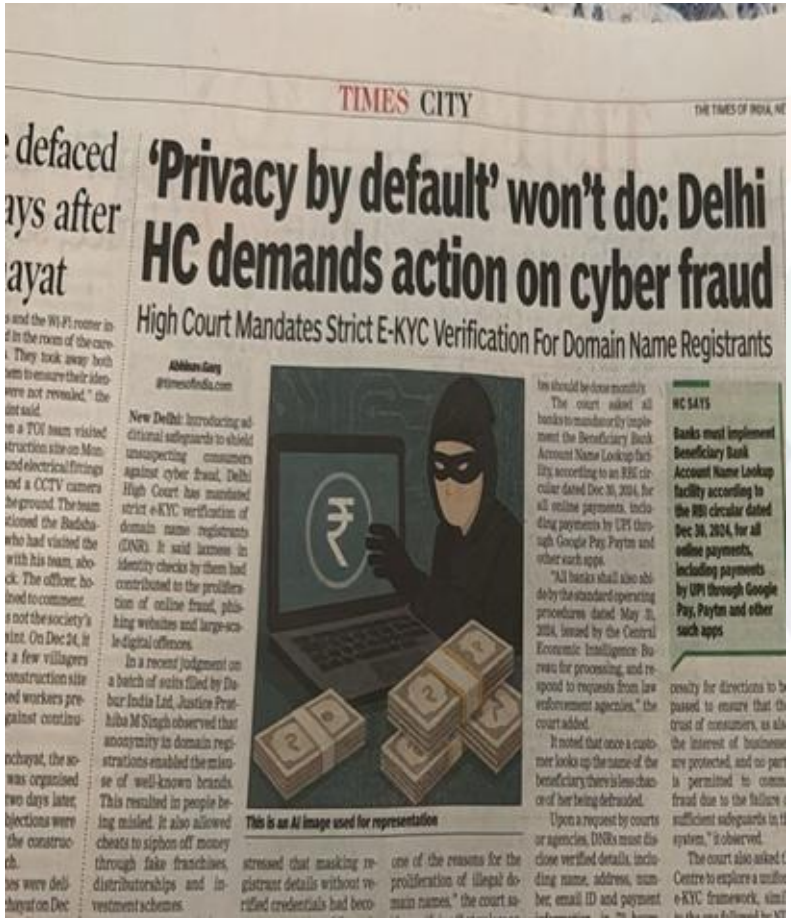
The new RAA has been approved and uploaded on the Registry website. Several new clauses have been incorporated to help reduce misuse of .IN domain names.

Key clauses include:

- Mandatory eKYC for all registrants.
- Maintenance of IP and financial transaction logs by registrars.
- Appointment of a Grievance Officer by each registrar.
- Appointment of a local representative with a registered office in India.

Outcome

High Court Mandates Strict e-KYC verification for DNRs



TIMES CITY

defaced
ays after
ayat

'Privacy by default' won't do: Delhi HC demands action on cyber fraud

High Court Mandates Strict E-KYC Verification For Domain Name Registrants

Abhinav Garg
@timesofindia.com

New Delhi: Introducing additional safeguards to shield unsuspecting consumers against cyber fraud, Delhi High Court has mandated strict e-KYC verification of domain name registrants (DNRs). It said laxness in identity checks by them had contributed to the proliferation of online fraud, phishing websites and large-scale digital offences.

In a recent judgment on a batch of suits filed by Dabur India Ltd, Justice Prathiba M Singh observed that anonymity in domain registrations enabled the misuse of well-known brands. This resulted in people being misled. It also allowed cheats to siphon off money through fake franchises, distributorships and investment schemes.

This is an AI image used for representation

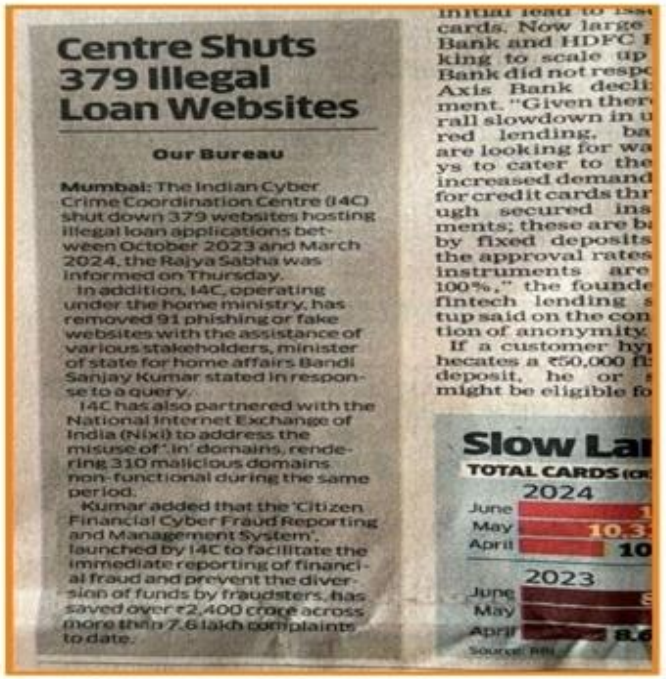
HC SAYS

Banks must implement Beneficiary Bank Account Name Lookup facility according to the RBI circular dated Dec 30, 2024, for all online payments, including payments by UPI through Google Pay, Paytm and other such apps

The Hon'ble High Court has appreciated the transparent and structured e-KYC procedure implemented by NIXI for domain name registrants.

The Court acknowledged that the process strengthens compliance, enhances transparency, and safeguards the interests of registrants within the digital ecosystem.

India LEAs appreciated NIXI's support



Centre Shuts 379 Illegal Loan Websites

Our Bureau

Mumbai: The Indian Cyber Crime Coordination Centre (I4C) shut down 379 websites hosting illegal loan applications between October 2023 and March 2024, the Rajya Sabha was informed on Thursday.

In addition, I4C, operating under the home ministry, has removed 91 phishing or fake websites with the assistance of various stakeholders, minister of state for home affairs Bandi Sanjay Kumar stated in response to a query.

I4C has also partnered with the National Internet Exchange of India (Nixi) to address the misuse of '.in' domains, rendering 310 malicious domains non-functional during the same period.

Kumar added that the 'Citizen Financial Cyber Fraud Reporting and Management System', launched by I4C to facilitate the immediate reporting of financial fraud and prevent the diversion of funds by fraudsters, has saved over ₹2,400 crore across more than 7.6 lakh complaints to date.

initial lead to last cards. Now large Bank and HDFC I king to scale up Bank did not respo Axis Bank decli ment. "Given ther rall slowdown in u red lending, ba are looking for wa ys to cater to the increased demand for credit cards thr ugh secured ins ments; these are b by fixed deposits the approval rates instruments are 100%," the founde fintech lending s tup said on the con tion of anonymity. If a customer hyp hecates a ₹50,000 fi deposit, he or might be eligible fo

Slow La
TOTAL CARDS (Cr
2024
June
May 10.3
April 10
2023
June
May
April 8.6
Source: RBI

"Between October 2023 and May 2024, 310 'malicious/phishing' domains have been made non functional with the help of NIXI. I4C has also collaborated with Industry for proactive detection of **phishing** websites on internet through technology-based solution. Further, 91 phishing/ fake websites and 379 illegal loan/scam apps hosting websites have been made non functional by I4C with the help of stakeholders concerned," he said.

THANK YOU