Preventing AI-powered domain name abuse

News & Updates • July 18, 2026

'First published on India Business Law Journal'

By: Madhu Rewari

Artificial intelligence (AI) has changed the internet in both useful and unsettling ways. It has improved search, accelerated customer service and expanded content creation. But it has also made abuse faster, cheaper and far easier to scale. One of the clearest examples is domain name abuse.

What once required time, technical skill and co-ordinated effort can now be executed at scale with generative AI, automation tools and synthetic content systems. If a fraudulent domain appears plausible, it can be the front door to phishing, malware delivery, counterfeit commerce, business email compromise, or impersonation fraud. AI has not created this problem, but it has made it far more efficient. Generative AI tools can produce convincing website copy, customer support scripts, product listings and multilingual phishing content in minutes. And the people behind these attacks are no longer technically skilled hackers working in isolation. They are increasingly what the cybersecurity community is beginning to call "bionic infringers", who combine the speed and scale of AI with human-curated deception. These are neither fully automated bots nor purely manual operations, but they are hybrid, making bionic infringers dangerous. They create fraud operations that are difficult to detect, expensive to fight and fast to redeploy when taken down.

Registrars and registries as infrastructure

This development raises an important question for the domain name ecosystem: what role should registrars and registries play in preventing and responding to abusive domain name activity?

Registrars (who sell domains) and registries (who manage top-level domains) serve as the foundation of internet governance. Their primary role is to enforce fair policies, identify and investigate threats early and take prompt, actionable mitigation measures, such as suspending malicious domains when presented with actionable evidence of domain name system abuse.

Their role can no longer be framed narrowly. Registrars and registries are not merely service providers, but are infrastructure actors.

NIXI deploys AI domain screening

AI-powered screening at the point of registration is the most significant shift registries can make. Rather than waiting for complaints to arrive after abuse has already harmed users, registries can build detection into the registration lifecycle itself. This means scanning domain names the moment they are created. The National Internet Exchange of India (NIXI), which manages the .in country code domain, has moved in this direction. At the ICANN85 Community Forum, hosted by the Internet Corporation for Assigned Names and Numbers (ICANN), held in Mumbai, NIXI presented a four-layered AI detection system built to identify fraudulent .in domains at registration.

In just six months of early deployment, NIXI reported that the system identified and neutralised more than 24,000 fraudulent websites, protected over two million users from potential fraud and reduced response times to under one hour from the moment a suspicious domain went live. One case study stood out: the system detected and blocked 143 fake State Bank of India websites before any victim could be targeted.

On 19 June on its 23rd Foundation Day, NIXI launched an AI-powered WHOIS screening platform, adding another layer to strengthen the verification and monitoring of domain registrations across India's internet ecosystem. The platform is designed to detect suspicious websites and bolster the integrity of domain data from the first step of registration.

Closing domain abuse structural gaps

For registrars, the equivalent responsibility lies in associated domain checks. Currently, when a registrar discovers that one domain in a registrant's account is being used for abuse, there is no obligation to investigate whether the same registrant has registered other domains as part of the same campaign. This is a structural gap that bad actors exploit, rotating through domain portfolios as individual names get taken down.

Shared intelligence across the ecosystem is the third pillar. Domain abuse is not a problem that any single provider can solve alone. When registrars, registries, security researchers and law enforcement share signals about abusive actors and registration patterns, the entire system becomes harder to exploit.

What NIXI's initiative demonstrates and what the global industry must take note of is that fighting AI-enabled abuse requires AI-enabled defence. That means AI-assisted screening, better verification, associated-domain analysis and stronger information sharing among registrars, registries, threat intelligence teams and law enforcement.

KEY CONTACT

Madhu Rewari

Partner

View Bio of Madhu Rewari