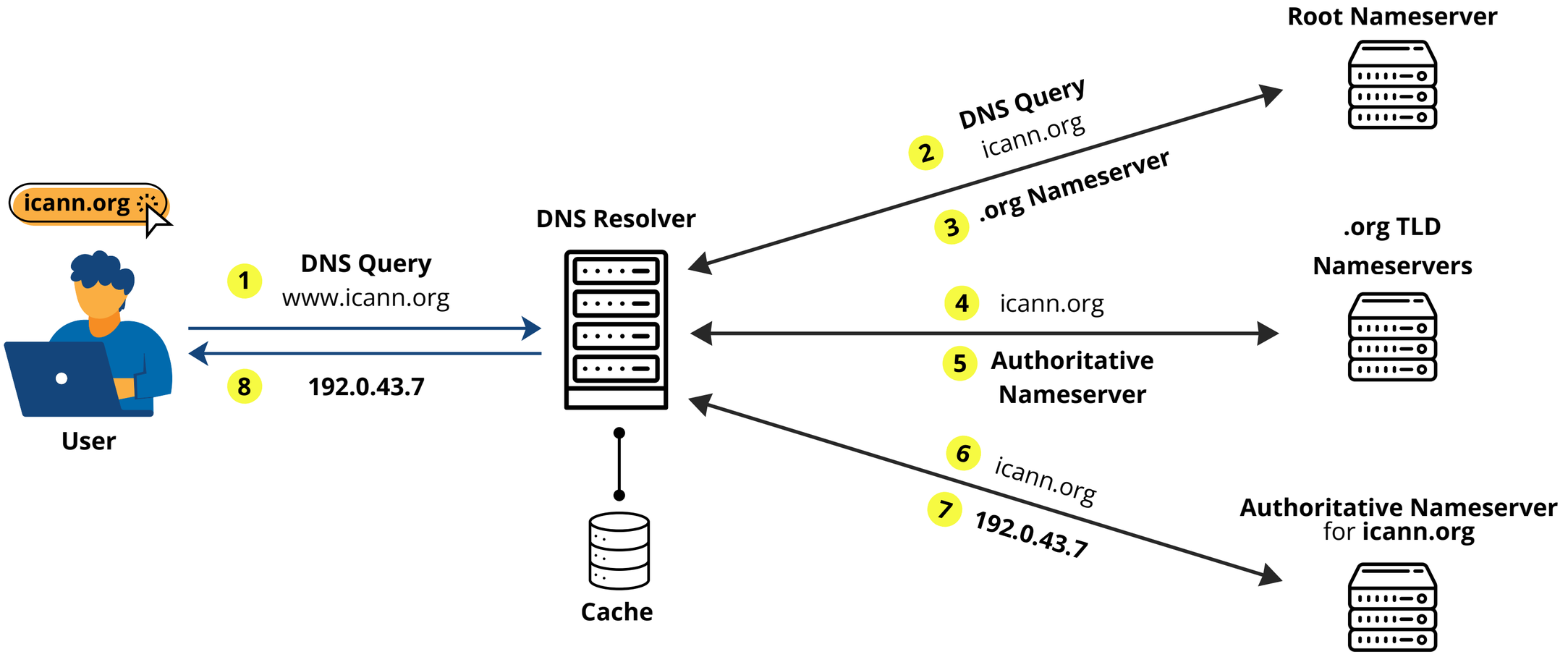
ICANN84, DUBLIN - 2025

CAN WE TRUST THAT WEB ADDRESS? STOPPING DNS ABUSE TOGETHER

Kushagra Singh
NextGen@ICANN84
National Forensic Sciences University, India

JOURNEY OF A WEB REQUEST



- DNS converts domain names into IP addresses
- ICANN coordinates the global Internet's unique identifier systems, including the DNS root and top-level domains, to help ensure the stable and secure operation of the Internet.

THE HIDDEN THREAT: DNS ABUSE

It's the technical misuse of domain names and the DNS infrastructure to cause harm.

- Phishing
- Malware
- Botnets
- Pharming
- Spam

FAKE WEBSITES (PHISHING)

MALWARE & BOTNETS

SPAM

PHARMING

WHY DNS ABUSE MATTERS

BREAKS DIGITAL TRUST

DNS abuse shatters the social contract of the internet, forcing users to constantly doubt the authenticity of every link they encounter.

MANIPULATING PEOPLE

The malicious domain name is merely the technical gateway; the true target is the user, manipulated through deception and fraud.

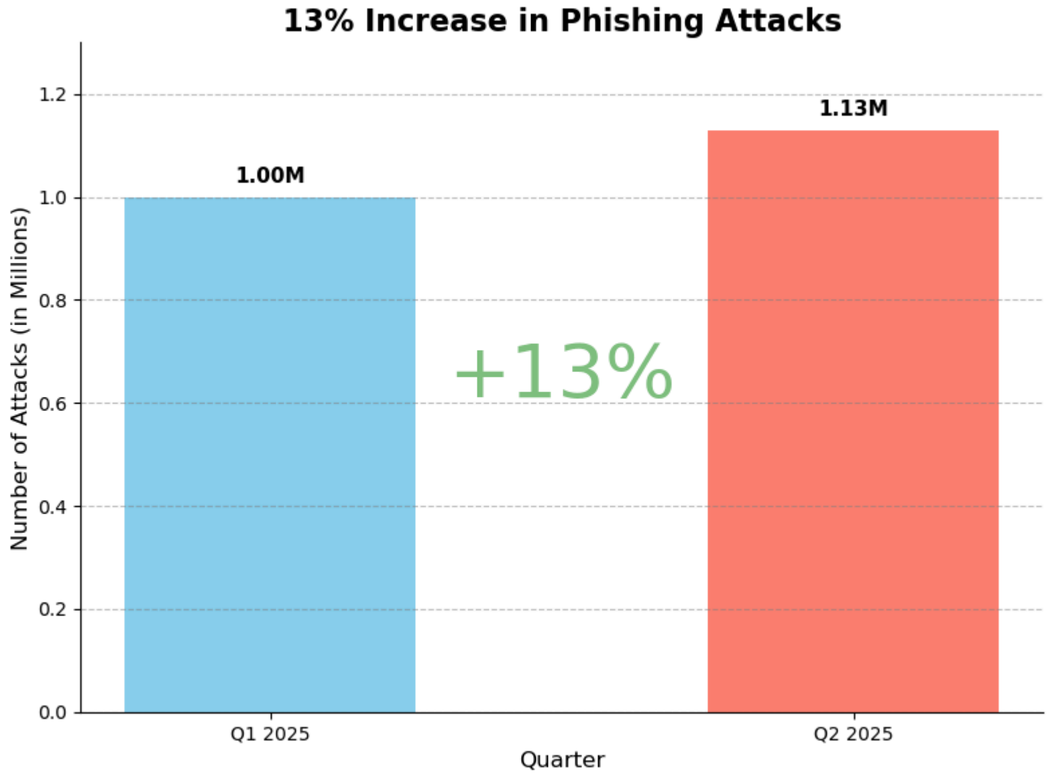
ENDING DIGITAL JOURNEYS

A single, costly scam or data breach can be enough to deter new internet users from engaging further with the digital world.

DNS abuse is large and concerning. NetBeacon reported 47,613 unique phishing domains in March 2025, about 87% of which were classified as maliciously registered.

IMPACT AND SCALE

- In underserved regions, awareness is low.
- Victims lose savings and confidence.
- When people lose money or data to fake domains, they don’t just lose trust ; they lose their digital confidence



1 in 174

DNS requests is malicious, a nearly six-fold increase from the previous year.

2.9M

malicious domains were detected over the last six months.

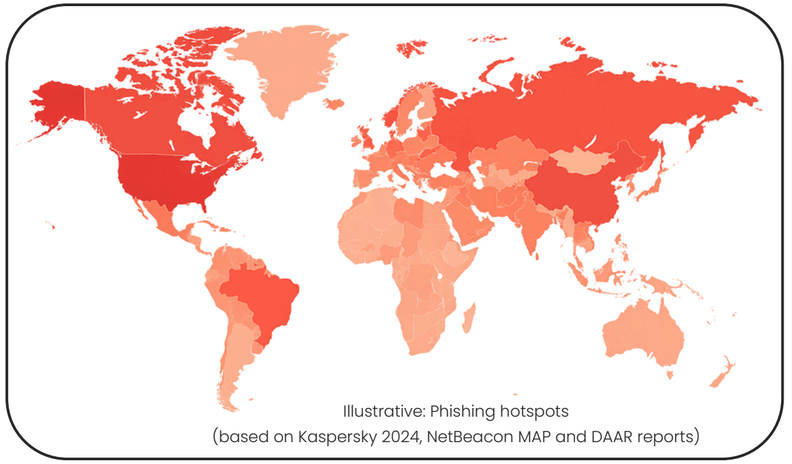
1.13M

phishing attacks were launched in Q2 2025, a 13% increase from Q1.

GLOBAL PICTURE

The New Tactic

Hijacking existing, legitimate domains to inherit their good reputation and evade detection.



Illustrative: Phishing hotspots
(based on Kaspersky 2024, NetBeacon MAP and DAAR reports)

The Data Shows a Clear Pivot :

- Use of compromised domains for Botnets: **+767%**
- Use of compromised domains for Phishing: **+62%**

The Challenge: The fight is no longer just about blocking "bad" domains, it's also about identifying "good" domains that are behaving badly.

WHAT'S BEING DONE

Policy & Enforcement :

- Contractual Obligations (2024): Binding obligations now in effect, resulting in over **2,700 domain suspensions** in the first 6 months.
- Smarter Measurement: The **DAAR** system has been retired and replaced by the new **ICANN Domain Metrica** for more advanced abuse tracking.

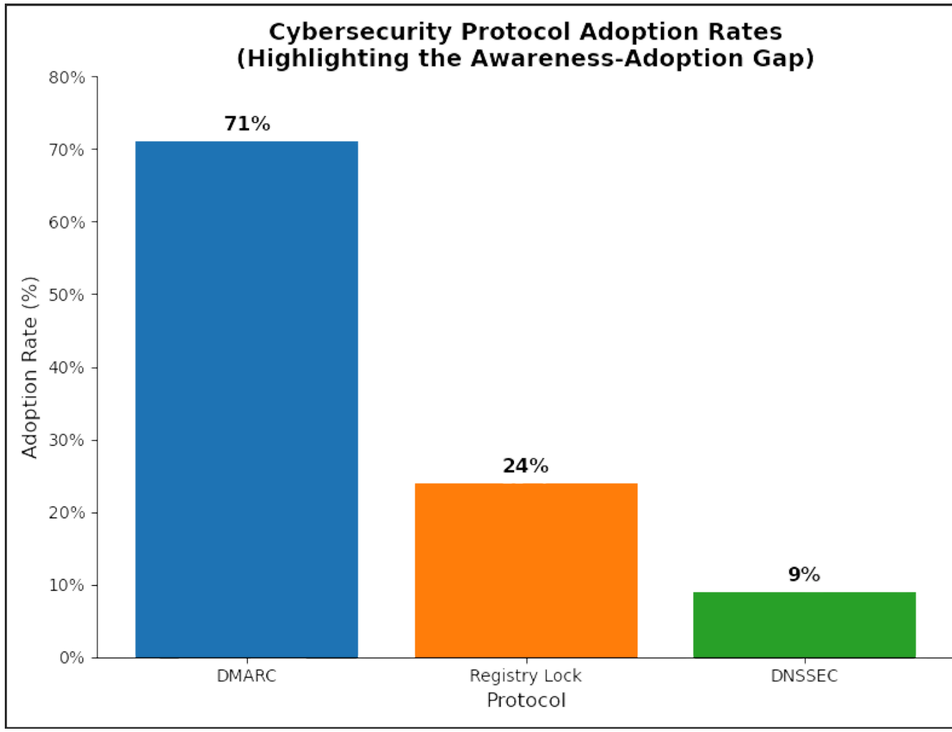
Industry Collaboration & Tools:

- NetBeacon Institute
- FIRST DNS Abuse SIG

Technical Toolkit :

There's a clear "Awareness-Adoption Gap" in using available tools:

- DMARC : **71%** Adoption
- Registry Lock : **24%** Adoption
- DNSSEC: **9%** Adoption



A CLOSER LOOK
DNS ABUSE MITIGATION IN INDIA

1. NIXI (.IN Registry) : Proactive Policy

- Mandatory **KYC** (know your customer) for .in Domains.
- **.bank.in** Initiative: Exclusive domain for Indian banks to boost trust and stop fake sites.

2. CERT-in : National Incident Response

- Coordinates response to major cybersecurity incidents like phishing and malware.

3. I4C : Law Enforcement & Awareness

- Helpline and citizen reporting portal.
- 'Cyber Dost' for public awareness.

nixi
Empowering Netizens

certin
Enhancing Cyber Security in India

CYBER
C D
DOST

PROACTIVE DEFENSE WITH AI/ML

Goal : Stop abuse before it happens.

Method 1 : AI at the Point of Registration

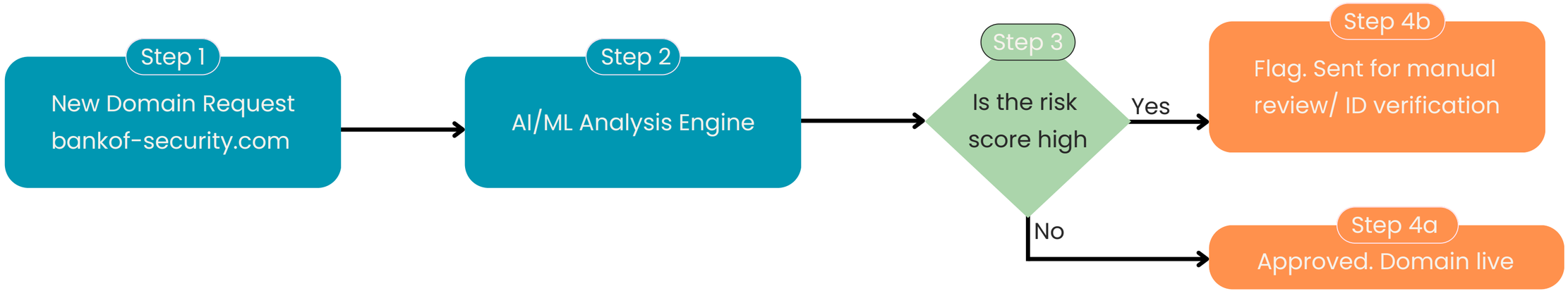
- Real-time analysis of new domain applications.
- Assigns a "risk score" based on key features.

DNS Belgium (.be)

SIDN (.nl)

Features Analyzed by AI :

- Lexical: **Typosquatting** (micrØsoft), **high entropy** (f8x9w3q.com).
- Reputation: **Domain age** (Newly Registered Domains are higher risk), registrar history.



AI FOR COVERT THREATS

Method 2 : Analyzing Live DNS Traffic

- Use Case : **Detecting DNS Tunneling**
  - Threat : Hiding data theft inside legitimate-looking DNS queries.
  - AI Solution : ML models **analyze traffic patterns** (query size, frequency, record types) to spot anomalies.
- Use Case : **Identifying Botnet DGAs**
  - Threat : Algorithmically-Generated Domains (AGDs) used by botnets to evade takedowns.
  - AI Solution : Deep learning models recognize the **pseudo-random patterns** of machine-generated domains.

WAY FORWARD

The Reality : DNS abuse is not just a technical issue; it's an **economic** and **social crisis** that erodes the trust our digital world is built upon.

The Strategy Shift : The fight is evolving. We must move from a reactive posture (blocking known threats) to a proactive, **AI-powered** strategy of **predicting and preventing** them.

The Required Actions (The 3 Pillars):

- Stronger Policy & Global Collaboration
- Smarter, Automated Detection Technology
- Greater User & Corporate Education (Awareness & Outreach)

THANK YOU

Kushagra Singh

@kushagrasinghh

kushagra.singh1501@gmail.com

References and Contact

Linktree