DNS Abuse Mitigation Tools in .id

IDADX

A collaborative, evidence-based approach at the .id registry

Ery Punta Hendraswara — PANDI .id Registry

ICANN86 Seville

Hello, we are PANDI – the .id Registry

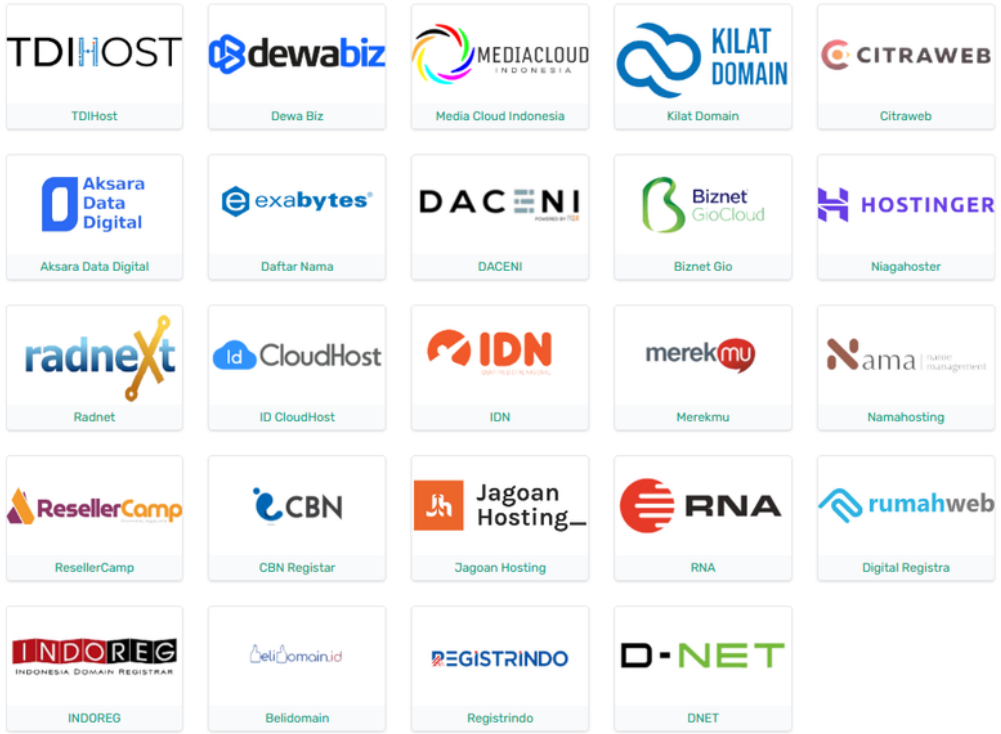
1.431.960

Domains Under Management · per 31 December 2025

.id · net.id · go.id · mil.id · co.id · my.id · sch.id · ac.id · web.id · ponpes.id · desa.id · biz.id

- **Non-profit legal entity since 2006**
- Manages the .id ccTLD since 2007; re-delegated by IANA in 2013
- **Multi-stakeholder governance**
  - Founding & independent members, government, internet industry, and academia

Registrar Ecosystem



The Abuse Challenge in .id - 2025

Total Reports Identified

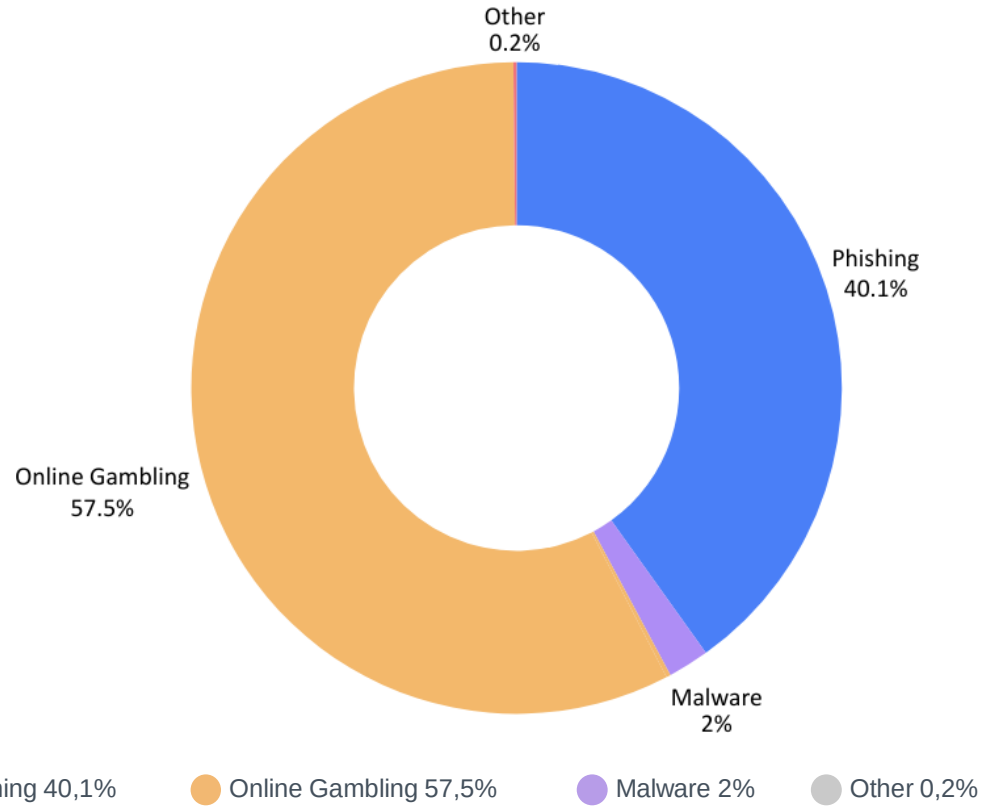
26.650

abuse reports across the .id ecosystem during 2025

Online Gambling – 57,5%
Illegal under Indonesian law · the dominant category

Phishing – 40,1%
The leading security-type abuse threat

Major Violation Categories



PANDI's Dual Mandate as a ccTLD

As the .id registry, PANDI must satisfy two layers of obligation — not only global abuse standards, but also Indonesian law and government instructions.

1 Global Abuse Standards

Technical DNS abuse per RAA / RA terms:

- Phishing
- Malware
- Botnets
- Pharming & Spam (as a vector)

2 National Legal Compliance

Content unlawful under Indonesian regulations & government instruction:

- Online gambling content
- Fraud & other unlawful content
- Material restricted by competent authorities

Policy basis: Section 6.4 of PANDI's Complaint Handling Policy — follow-up & coordination with the Ministry of Communication and Digital Affairs (Komdigi) and competent authorities; suspend / unsuspend through a documented process.

How IDADX Works

IDADX (Indonesia Anti-Phishing Data eXchange) is PANDI's system for handling .id domain abuse. Reports from many sources are pooled, then registrants and registrars are notified automatically — with handled cases published publicly at **idadx.id**.

1 Collect
Reports & data on .id abuse pooled from many sources (incl. internal crawling)

2 Correlate
Indicators matched & evidence enriched against the registry record

3 Auto-Notify
Email sent automatically to the Registrant & Registrar on WHOIS / RDAP

4 Enforce
Content removed in time, or the domain is suspended per the matrix

5 Publish
Handled domains listed transparently on idadx.id

Two automatic notifications from IDADX

1. Warning + take-down instruction
Registrant must remove the content within the response window (no window for Autosuspend cases).

2. Suspension notice
Confirms the .id domain has been suspended by PANDI under the applicable category.

Recovery: Registrants can request **unsuspend** or domain **whitelisting** via the PANDI form or **helpdesk@pandi.id**.

A Multi-Party Collaboration Ecosystem

Reports reach IDADX from three streams — government partners, external intelligence, and PANDI's own internal crawling — producing standardized, evidence-backed action across the .id ecosystem.

Government of Indonesia

Regulatory authority & national-security coordination

Komdigi
Ministry of Comms & Digital

BSSN
National Cyber & Crypto Agency

External Sources & Intelligence

Threat intelligence & trusted notifications

Each contributes as one of several trusted notification sources

BIMA — PANDI's internal crawling engine
Breach Identification & Monitoring Assistant proactively crawls .id domains to detect violating content, feeding findings directly into IDADX alongside external and government inputs.

Mechanism for Handling Abuse

Handling Workflow

1. **Report Received**
2. **Validate & Classify**
3. **Notify Registrar / Registrant**
4. **Registrant Remediation**
5. **Enforce (Suspend)**
6. **Verified Correction (Unsuspend)**

Suspension Categories

Category	Abuse Criteria
Autosuspend	my.id / biz.id / web.id infiltrated with negative content; content is on the registered primary domain (not a subdomain); and domain age is less than 60 days.
Autosuspend **1 × 24 hours**	my.id / biz.id / web.id infiltrated with negative content; and domain age is less than 60 days.
Autosuspend **3 × 24 hours**	my.id / biz.id / web.id infiltrated with negative content and domain age is more than 60 days.
Manual **Suspend**	Extensions other than my.id / biz.id / web.id that are infiltrated with negative content.

"Negative content" = content unlawful under Indonesian regulations or flagged by competent authorities.

Thank You.

Let’s Connect

pandi_id | domaindotid **pandi.id | domain.id**