Domain Name Abuse Strategy for .nz

DRAFT v 0.3

Contents

About this document

InternetNZ, working with the Domain Name Commission, is developing a strategy to guide our work in addressing domain name abuse of domain names in the .nz domain space.

The Domain Name Abuse strategy is operational, which means it will guide the work of InternetNZ and the Domain Name Commission, aligning the annual work programme planning of .nz Rules and InternetNZ and Domain Name Commission. In some cases, .nz Rules changes may be required to bring effect to the suggested direction in the strategy.

This strategy has been approved as the 'In Principle' direction by the InternetNZ Board. The ultimate outputs of this strategy will be achieved by our mandated Policy Development Process through engagement with the local Internet Community on amendments to the .nz Rules or through introducing operational policies.

Introduction

The concept of abuse of domain names is broad, covering technical abuse of domain names (for example, phishing attacks and delivery of malware) and website content abuse (facilitating access to illegal content or using the domain name for criminal and/or illegal conduct).

The .nz Rules that govern the .nz country code top-level domain (ccTLD) have long included a provision that InternetNZ is not concerned with the use of domain names. In addition, the current .nz Rules prevent the Domain Name Commission from acting on a complaint about activities in domain name use, including complaints about phishing, malware, and objectionable content, except in exceptional or emergency circumstances. However, many industry stakeholders believe the InternetNZ Group has the potential to play a limited yet important role in addressing abuse in the .nz domain.

Concerns are rising as advancements in technology allow for more complex deceptions (i.e., deep fakes), with financial fraud activities being corporatised and operationalised by sophisticated criminal syndicates. In response, multiple industries are responding to protect consumers and combat financial crimes, including banks, telcos, payment systems, and digital service providers.[1]

Internationally, 'no concern for use' policies are now uncommon among country-level domain name registries, and most similarly-situated providers allow for a degree of Domain Name System (DNS)-level intervention in order to address illegal activity.[2] A

[1] See the 2025 GASA State of Scams report.
[2] See Online Harm and Domain Name Operator Policies: A report produced for the InternetNZ Group by Mark Boddington (July 2023)

2020 review of the .nz Rules noted this international context, and recommended that the .nz Rules should reflect that illegal activity requires intervention by the .nz manager.[3]

This strategy seeks to clearly outline the areas where InternetNZ and the Domain Name Commission will focus their efforts to address illegal activity in the coming years and the types of initiatives that will support it.

Through operationalising this strategy, InternetNZ will identify:

- In what circumstances it's appropriate for the Domain Name Commission or the .nz registry to intervene directly
- What thresholds and guardrails provide parameters to refresh our policy framework
- How tools, processes, and procedures support operationalising our longer-term approach
- Where partnership, information-sharing or referrals might be a preferable course of action.

Overall outcomes of the strategy

The strategy supports InternetNZ Group's vision of "A fair and inclusive Internet for Aotearoa New Zealand, where the trusted .nz brand drives social and economic value."

The strategy contributes to two strategic pillars ("Service Excellence" and "Future Sustainability & Growth") and their goals within the 2026-31 InternetNZ Group strategy. Taking a 5-year operational approach to systematically mitigate illegal activity ensures trust in the .nz domain name space remains strong, is foundational to business growth, and aligns with our aim to continuously improve our service delivery.

The strategy will bring into effect the .nz Principles that guide the management of .nz. These Principles[4][5] are:

- .nz should be **secure and trusted**: .nz infrastructure must be dependable and secure, and .nz be trusted
- .nz should be **open and accessible**: everybody should be able to observe, participate, innovate and enjoy the benefits of .nz
- .nz should **serve and benefit New Zealand** and reflect and be responsive to our diverse social, cultural and ethnic environment

[3] Re-imagining the future of .nz: Recommendations Report of the .nz Advisory Panel (2020, page 19)
[4] .nz Rules, version 3.1 (1 July, 2025)
[5] Noting that the .nz Principles must be taken as a whole and any tensions between them carefully balanced. No principle is dominant over another.

- .nz should **support te reo Māori me ōna tikanga** and participation in .nz by Māori[6]
- .nz should **enable New Zealand to grow and develop**: it should help people, businesses and organisations connect, create, innovate and grow.

The strategy also reflects InternetNZ's constitutional commitment to an open, global, interoperable Internet. To that end, this strategy proposes that it is necessary to enable DNS-level interventions in relation to some abusive and illegal use of domain names. This approach is consistent with InternetNZ's other constitutional commitments of contributing to a resilient and secure Internet and maintaining the .nz domain name space to meet local and international standards.[7]

Summary of focus areas

InternetNZ and the Domain Name Commission will prioritise the following work to enhance the trust in .nz, and disrupt scams and fraud:

- **Registration abuse** — Undertaking activities to ensure accurate registration information is provided on registration of domain names, and
- **Technical abuse** — Pursuing .nz Rules changes to enable us to act on evidenced technical abuse (e.g. phishing and malware) because it impacts trust in, and the security of, the .nz domain.

These focus areas also reflect that phishing facilitates online fraud and scams. Phishing, along with scams and fraud, have been identified by the Domain Name Commission as the most reported problems in the .nz domain name space[8] and are risks to the safety and trust in the .nz domain space. It is also well known that the use of inaccurate registration information (often referred to as registration abuse) is closely associated with malicious and illegal use of domain names.

We also propose investigation of DNS-level intervention to respond to criminal content online. This will include exploring the potential to join or develop Trusted Notifier networks; considering what threshold of criminal/illegal conduct should be acted on; examining what process safeguards need to be in place; and determining how complaints and appeals can be handled.

---

[6] NB: this is a draft principle

[7] https://internetnz.nz/governance-and-reports/governance-documents/internetnz-constitution/

[8] Suspensions of domain names in the last year have primarily been where domain name holders will not confirm their registration data and reports have been received of alleged phishing, brand impersonation and fake webshops.

The first priorities for responding to criminal content will be to:

- Consider a mandate to act to directly disrupt Child Sexual Abuse Material (CSAM) content, which is universally accepted as abhorrent and for which there is an established globally recognised Trusted Notifier.[9]

- Ensure that, where InternetNZ does not have a mandate to act, it can play its part by referring matters out to the appropriate or responsible agencies.

The ecosystem of domain name malicious use

Across the global domain name system, domain name Registries and their compliance functions are facing similar issues and core policy questions:

- What defines and constitutes "DNS Abuse"?
- When should a registry or the regulator act?
- And under what authority and evidentiary standard?

While definitions and intervention thresholds differ globally, the following five models illustrate the spectrum of responsibility that InternetNZ might learn from.

International Precedents

1. *ICANN gTLD Model*: Focuses on gTLDs, narrow technical definitions of DNS abuse (phishing, malware), has acceptable use policies, and enforces through contractual obligations.
2. *auDA (.au) Model:* Leverages Australian presence requirements. Has a national Scam Prevention Framework, proactively engages with national safety bodies to mitigate DNS abuse, and collaborates closely with government and industry, including government run National Scams Centre.
3. *Nominet (.uk) Model:* Utilises a bifurcated system: formal Dispute Resolution Service for rights disputes, and a separate criminal investigation process with enforcement agencies through a formal partnership policy and training for agency partners. Noting each agency makes the formal decision to intervene and directs the registry to action it.
4. *CIRA (.ca) Model:* Leverages Canadian Presence Requirements to validate registrants and reduce DNS abuse, combining policy with verification mechanisms.
5. *PIR (.org) Model:* Operates internationally and responds to technical abuses and limited categories on website content abuse.[10]

[9] The Domain Name Commission already has a referral out mechanism in place with the Department of Internal Affairs but no mandate to act directly to respond to CSAM complaints.
[10] https://pir.org/our-impact/anti-abuse-policy/

The international landscape highlights that there is no single “best practice”. Rather, there is a continuum of responses between strict neutrality and proactive intervention. Each model reflects local jurisdictional and legal mandates, public expectations, and the maturity of their ecosystem partnerships.

New Zealand Landscape

New Zealand’s online safety and cyber resilience ecosystem is defined by distributed responsibilities across multiple agencies and entities. Each operates under distinct statutory mandates and operational constraints. There are limited takedown provisions in New Zealand legislation under which Government agencies can act to disrupt criminal activities.

The .nz registry and Domain Name Commission sit adjacent to these agencies, with strong collaborative potential but no strong, formal enforcement role beyond the .nz Rules.

- *National Cyber Security Centre (NCSC):* Operational lead, Phishing Disruption Service, potential trusted notifier for rapid threat identification.
- *Netsafe:* Focused on individual harm under the Harmful Digital Communications Act, limited statutory role, receives numerous scam reports.
- *New Zealand Police:* Investigates cyber-enabled crimes, criminal justice processes need to ensure due process and very high evidential standards - not well aligned with rapid takedowns.
- *Department of Internal Affairs (DIA):* Manages objectionable content and Unsolicited Electronic Messaging and collaborates effectively with the Domain Name Commission as the moderator of .govt.nz (ensuring the govt.nz namespace is appropriately managed).
- *Financial Markets Authority (FMA):* Principal conduct regulator for financial markets and has a key role in regulating investment products.

The New Zealand landscape has some unexplored jurisdictional gaps. An observed policy tension is that most entities need to balance the speed of response with appropriate due process.

DNS-level responses

The tools available at a DNS-level to address malicious use include the ability to suspend, cancel, redirect and transfer a domain name.[11] In general, DNS-level tools are considered a blunt instrument[12] to be used only when other options are unavailable, and this will be reflected in the strategy. Checks pre-registration can

[11] For the .nz domain, any DNS-level intervention must be carried out in line with the .nz Rules. At present these allow for intervention in limited cases.
[12] Explainer - https://www.youtube.com/watch?v=kVwKDq-qUwY

often avoid later DNS-level interactions. DNS-level responses are sometimes considered appropriate where there is illegal activity and high harm, and the response is considered proportionate relative to any collateral damage.[13]

DNS-level responses also need to consider more complex use cases, such as shared hosting sites or exploited domain names, where interventions may have unintended consequences for subdomains, other domain name holders or the domain name holder.[14]

In addition to discussion of DNS-level levers, other actions to address abuse, including activities carried out in collaboration with other actors in the ecosystem, such as referral processes or as provided for in Trusted Notifier agreements[15]. Supporting actions may also include transparency reporting, participating in intelligence reporting networks[16], or education for domain name holders.

Consideration of the threshold for action by the Domain Name Commission or the Registry needs to be aligned to the type of intervention, and whether that intervention needs to be different for different levels of activity — illegal acts vs criminal acts vs acts of deception.

It is noteworthy that trusted parties have recently emerged who can provide 'high certainty' evidenced reports of phishing and malware associated with a domain name. They are also able to eliminate 'compromise' concerns by distinguishing between malicious or compromised domain names.[17]

The International Watch Foundation is able to provide trusted reports that a domain name is being used for the distribution of CSAM, and that the domain name has no secondary valid purpose/is not being exploited or compromised.

The table below outlines some of the potential approaches that could be in scope. Any interventions to counter malicious use will need to be clearly scoped and reflect InternetNZ's role as registry operator and Domain Name Commission's role as regulator for .nz. Noting adjacent functions in the ecosystem, such as the monitoring

[13] For more detail of recommended considerations, see the Internet & Jurisdiction Policy Network Toolkit 'DNS Level Action to Address Abuses'.
[14] For example, a single IPv4 address may represent hundreds or even thousands of users due to widespread use of Carrier-Grade Network Address Translation (CGNAT), VPNs and proxy middleboxes
[15] Such as Nominet's Criminal Practices Policy. See the the related annual report - https://nominet.uk/wp-content/uploads/2025/05/Nominet-2024-Criminality-Report.pdf
[16] Noting that the New Zealand Anti-Scam Alliance is working to strengthen anti-scam efforts and support collaborative efforts focusing on preventing, detecting and disrupting online financial scams across banking, telecommunications, and digital platforms.
[17] That is, where a domain name is the victim of hacking or exploitation and take down is not an appropriate response.

and enforcement of legislation (for example), sit with the Police and other government agencies.

Types of tools

Working with others in the ecosystem	DNS-level proactive .nz Rules enforcement actions	DNS-level reactive .nz Rules enforcement actions
• Refer-on notifications of abuse to the relevant regulator (content abuse) • Refer takedown requests to hosting providers or registrars as appropriate • Working with other actors (e.g. enforcement agencies, registrars, trusted notifiers/verifiers, domain name holders) and supporting policies/agreements	• Risk-based enforcement of registration rules, potentially leading to suspension or cancellation if requirements not met (current Domain Name Commission approach) • Increased due diligence relating to identification of domain name holder at time of registration of domain names	• Disputed names process (for example Intellectual Property abuse in domain names managed under the Dispute Resolution Scheme — current approach) • Use of DNS-level tools like suspension or cancellation in limited circumstances (for example, when DNS abuse is proven or pursuant to Court order or lawful request of authorised agency or trusted notifier.)
Any use of these tools would need to be supported by the Domain Name Commission's Regulatory Approach, the .nz Rules, and appropriate technical and system capabilities, adequate resourcing and processes.		

Stakeholder feedback

As part of developing this strategy, we sought feedback from a range of key stakeholders. In particular, hearing what protections were needed to ensure interventions are appropriate (what Guardrails should be in place) and hearing what the priority focus should be.

It was acknowledged that scams and fraud are of high concern for consumers and also impact the trust in domain name spaces. Private actors and NGOs are increasingly taking more responsibility to disrupt fraud, as is demonstrated by the activities of the Anti-Scam Alliance[18]. Some Government agencies acknowledge that

[18] https://www.mbie.govt.nz/about/news/new-zealand-anti-scam-alliance-launched-to-strengthen-scam-prevention-efforts and https://www.beehive.govt.nz/sites/default/files/2025-07/Anti-scam%20Alliance%20report_0.pdf

their response to criminal activity is limited, as they do not have timely methods of responding to scams and fraud.

We heard from all stakeholders that there is a role for InternetNZ and the Domain Name Commission to sensibly disrupt scam activities. The most effective and timely way of achieving this was commonly identified to be through adding friction (verification of identity) to the registration process, and is an approach other ccTLDs are taking.

Stakeholders noted the importance of .nz maintaining high standards so that it is not targeted due to perceived immature disruption modalities relative to developing global practices. It was also observed that whilst .nz should be trusted and secure in and of itself for all users, that domain name holders and registrars benefit where high trust exists in .nz.

Most stakeholders believed that InternetNZ and the Domain Name Commission should not judge illegal content and that developing relationships with trusted notifiers would be a preferable approach. We cemented our confidence that trusted notifiers currently exist to allow for high certainty action in respect of domain names being used for delivery of phishing, malware, and CSAM.

Our proposed approach

Guardrails needed to support any intervention

Interventions to address domain name abuse should be undertaken in line with the following list of guardrails, to ensure actions are fair and appropriate.

1. **Intervention proportionate to the risks**, which includes having clear frameworks and processes for intervention for different types of abuse, and maintaining a clear understanding of the current and emerging risks in relation to DNS abuse on .nz
2. **Clarity around InternetNZ's role**, which includes having transparency about InternetNZ Group's mandate to address domain name abuse in .nz and its regulatory function, and the opportunities for community consultation.
3. **Risks of incorrect decisions minimised**, ensure there are adequate safeguards to prevent wrong decisions (notice periods/opportunity to seek reversal of decisions) and a clear, responsive complaints process for domain name holders impacted by a decision.

First focus — disrupting scams and fraud

It is proposed that the initial focus will be addressing scams and fraud facilitated by DNS abuse in the .nz domain space.

Fraud and scams have been identified as a significant problem for New Zealanders.[19] Fake webshops are of particular concern — these can involve phishing scams that impersonate webshops in order to extract personal information from users. Fake webshops and other scams are common, difficult for the public to detect, and cause harm and disruption for many internet users.

Currently, the Domain Name Commission has limited options for acting quickly on fraud and scams, and Courts are not responsive enough to address this quick-moving challenge. We consider the prevalence of fraud and scams to be a threat to the integrity, security, and reputation of the .nz domain space.

In line with where the industry is going internationally, the methods we will investigate introducing to address scams and fraud are increased registration checks and disrupting scam activities by acting on evidenced phishing and malware reports.

We will also closely follow ICANN's current work looking at the role that high volume registrations play in facilitating DNS abuse — and whether there should be more friction to rate limit registrations.[20]

Having fraud and scams as the first focus areas for the strategy will enable InternetNZ and the Domain Name Commission to work through different options for action as part of a holistic roadmap of change. Relevant to this focus area will be the work of the Government who is supporting the disruption of scams through the New Zealand Anti Scam Alliance and also looking to introduce legal protection (a Safe Harbour) to protect good faith action for disrupting scams.

Regcheck – A potential tool

One emerging method of disrupting domain name abuse is a Regcheck process, which holds a domain name out from the zone where signals/intelligence indicate that a newly registered domain name is registered with fake information (amounting to Registration abuse) or where there are strong indicators that it may be used maliciously.

It is proposed that InternetNZ consider implementing a targeted minor delay in registration to undertake registration checks on high risk domain name registrations so as to reduce the harm that can be caused even by a short period in the zone.

It is noted that Cybersecurity legislation in the EU (known as NIS-2) places obligations on the regulated industry (those providing services in the EU) to ensure data is accurate and that verification of the identity of the user is undertaken. This has led to many providers introducing greater checks at registration, and lower abuse complaints are being observed.

---

[19] See the 2025 GASA State of Scams report.
[20] https://itp.cdn.icann.org/en/files/generic-names-supporting-organization-council-gnso-council/preliminary-issue-report-on-a-pdp-on-dns-abuse-08-09-2025-en.pdf

Second focus — Other criminal activity and trusted notifiers

InternetNZ and the Domain Name Commission are not capable or qualified to judge illegal content. The majority of equivalent ccTLDs will only act on criminal conduct if directed to by Court Order or following a takedown direction from an empowered agency. Nominet is one example of a ccTLD that acts under a Criminal Practices Policy in partnership with Government.[21] Our community were in favour of acting on reports of trusted notifiers when consulted by an independent panel in 2020.[22]

It is not clear, at this time, whether there are any Government agencies that would seek to act as trusted notifiers, or whether a referral out process should be used instead, under which reports of illegal activity are referred out by InternetNZ/the Domain Name Commission to the appropriate Government agency for action.

As part of our work, we propose further investigating DNS-level intervention avenues to respond to criminal content online. This will include looking into the feasibility of developing a trusted notifier/partner network; considering what threshold of criminal/illegal conduct should be acted on; examining what process safeguards should be in place; and determining how complaints and appeals can be handled.

The first priority for responding to criminal content will be to consider a mandate to act to disrupt CSAM content, which is universally accepted as abhorrent and for which there is an established, globally recognised trusted notifier.

Where InternetNZ does not have a mandate to act, a clear process for referring matters out to responsible agencies and/or providing information to victims/complainants would need to be developed.

In addition to that initial focus area, it is proposed that the InternetNZ Group keep a watching brief on other emerging threats and risks.

[21] https://nominet.uk/wp-content/uploads/2025/03/Criminal-practices-policy.pdf
[22] https://internetnz.nz/assets/Archives/dotnz-policy-review-overview-of-submissions.pdf (page 64-68).