This document is a preview of the 2nd edition of the DASC survey.
To participate in the survey, go to https://www.surveymonkey.com/r/2024DASC
Read more here: https://ccnso.icann.org/en (Go to "highlights")

---

ccTLD DNS Abuse Survey

Page 1. WELCOME

Welcome to the 2nd survey by the ccNSO DNS Abuse Standing Committee (DASC). Thank you for participating in our survey.
Conducted in August - September 2024, this survey follows up on the initial survey from Q4 2022. Read more here: https://ccnso.icann.org/en (Go to "highlights")

DISCLAIMER

This survey is for ccTLDs only. Please submit only one (1) response per ccTLD.

We want to assure you that all responses collected are confidential. Your responses will be anonymized and aggregated with those of other participants to analyze trends and patterns. Any identifying information provided will be kept separate from the survey responses and will not be shared with any third parties.

The ccNSO DASC thanks you for your cooperation. If you have questions, please contact the ccNSO Secretariat at ccnsosecretariat@icann.org

1. *Multiple Choice*
   I agree that my personal data will be processed in accordance with the ICANN Privacy Policy (https://www.icann.org/privacy/policy), and agree to abide by the website Terms of Service (https://www.icann.org/privacy/tos). *
   - ☐ Yes
   - ☐ No (Selecting this answer option will end the survey)

2. *Multiple Choice*
   I am answering this question on behalf of an organization or entity responsible for managing a ccTLD, which is listed as such in the IANA Root Zone Database. *
   - ☐ Yes
   - ☐ No (Selecting this answer option will end the survey)

Page 2. RESPONDENT DATA

3. *Comment box*

Please specify the ccTLD(s) you represent. This also includes IDN ccTLDs. Use a comma to separate if more than one.*

4. *Comment box*
   We encourage you to specify your e-mail address (optional). Note that this address will not be shared with anyone, but might be used by the DASC survey team in case of questions.

5. *Multiple Choice*
   Please select the ICANN geographical region for your ccTLD. *
   - ☐ Africa
   - ☐ Asia/Australia/Pacific
   - ☐ Europe
   - ☐ Latin America/Caribbean islands
   - ☐ North America

6. *Multiple Choice*
   Please select the governance model for your ccTLD.
   - ☐ Academic institution
   - ☐ For profit company
   - ☐ Governmental institution
   - ☐ Not for profit organisation
   - ☐ Other (please specify)

7. *Checkboxes*
   Which registration model do you follow? Please select all that apply.
   - ☐ 3R: Registry-Registrar-Registrant model
   - ☐ Direct registrations
   - ☐ Other (please specify)

8. *Multiple Choice*
   What is the number of domains under management for your ccTLD? Please select the appropriate range.
   - ☐ 0 to 5000

- ☐ 5,001 to 10,000
- ☐ 10,001 to 50,000
- ☐ 50,001 to 100,000
- ☐ 100,001 to 1 million
- ☐ more than 1 million

9. *Multiple Choice*
   How many employees (Full Time Equivalents) does your ccTLD have? Please select the appropriate range.
   - ☐ 1
   - ☐ 2 to 5
   - ☐ 6 to 10
   - ☐ 11 to 30
   - ☐ 31 to 50
   - ☐ more than 50

10. *Multiple Choice*
    My ccTLD has a DNS Abuse Officer as part of the registry.
    - ☐ Yes
    - ☐ No
    - ☐ Not sure
    - ☐ Other (please specify)

11. *Multiple Choice*
    Data Protection legislation affects my ccTLD registry function. Note: This question does not refer to HR matters
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

Please explain

12. *Multiple Choice*
    If you provide services to registrars, what is the average domain name registration price your ccTLD charges its registrars?
    - ☐ Less than 5 USD
    - ☐ Between 5 and 10 USD

- ☐ Between 10 and 20 USD
- ☐ Between 20 and 99 USD
- ☐ More than 99 USD
- ☐ Not applicable
- ☐ Other, please specify

13. *Multiple Choice*
    If you provide services directly to the public, what is the average domain name registration price your ccTLD charges the public?
    - ☐ Less than 5 USD
    - ☐ Between 5 and 10 USD
    - ☐ Between 10 and 20 USD
    - ☐ Between 20 and 99 USD
    - ☐ More than 99 USD
    - ☐ Not applicable
    - ☐ Other, please specify

14. *Multiple Choice*
    There were recent amendments to the base generic top-level domain (gTLD) ICANN Registry Agreement (Base RA) and the 2013 ICANN Registrar Accreditation Agreement (RAA) related to DNS Abuse. Has your ccTLD adopted them?
    - ☐ Yes
    - ☐ No
    - ☐ Not currently, but planning to
    - ☐ Not sure

Page 3. TYPES OF ABUSES

15. *Checkboxes*
    My ccTLD takes DNS Level Action against the following types of abuse. Please select all that apply.
    - ☐ Technical abuse (e.g. Malware, botnets, phishing, pharming, spam)
    - ☐ Problematic website content (e.g. child abuse material, violent extremist content, hate speech, intellectual property infringements, controlled substances and regulated goods for sale or trade)
    - ☐ Trademark infringements in the domain name (e.g. homographs, typosquatting, cybersquatting, domain kiting)
    - ☐ Other, please specify

16. *Multiple Choice*
    Approximately what % of domains do you believe are subject to DNS Abuse in your ccTLD? Please select the appropriate range.
    - ☐ Less than 0.05%
    - ☐ Between 0.05% and 0.1%
    - ☐ Between 0.1 and 0.15%
    - ☐ Between 0.15 and 0.20%
    - ☐ More than 0.20%
    - ☐ Not sure

17. *Checkboxes*
    Against which of these types of technical DNS abuse does your ccTLD take action? Please select all that apply.
    Source of the definitions below: SAC115.
    https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf
    - ☐ MALWARE. Malware is malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
    - ☐ BOTNETS. Botnets are collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.
    - ☐ PHISHING. Phishing occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end-users to copycat websites. Some phishing campaigns aim to persuade the user to install malware.
    - ☐ PHARMING. Pharming is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking can occur when attackers use malware to redirect victims to the perpetrator's site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false Internet Protocol (IP) address bearing malware. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.
    - ☐ SPAM. Spam is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.
    - ☐ None
    - ☐ Other (please specify)

18. *Checkboxes*
My ccTLD takes DNS Level Action when illegal content is detected. Please select all that apply.
    - ☐ Yes, we take proactive action based on complaints or our own intelligence/ investigation
    - ☐ Yes, we take action if we receive instructions from a regulatory and/or enforcement authority
    - ☐ No, we do not take action (by selecting this answer option, you automatically skip question 19)

19. *Comment box*
My ccTLD takes DNS Level Action against the following types of website content abuse. (Examples may include, but are not limited to, disinformation, child abuse material, violent content, hate speech, intellectual property infringements, controlled substances and/or regulated goods for sale or trade) Please list all that apply.

20. *Checkboxes*
My ccTLD takes DNS Level Action when child sexual abuse material (CSAM) is detected. Please select all that apply.
    - ☐ Yes, we take proactive action based on complaints or our own intelligence/ investigation
    - ☐ Yes, we take action if we receive instructions from a regulatory and/or enforcement authority
    - ☐ We act upon Internet Watch Foundation (IWF), INHOPE, NMEC or equivalent notifications
    - ☐ No, we do not take action

21. *Checkboxes*
My ccTLD takes DNS Level Action when ***content*** abuse related to trademark infringements is detected (ie the domain links to a fake webshop but the domain itself does not imitate a trademark). Please select all that apply.
    - ☐ Yes, we take proactive action based on complaints or our own intelligence/ investigation
    - ☐ Yes, we take action if we receive instructions from a regulatory and/or enforcement authority
    - ☐ No, we do not take action unless required to under a court order (by selecting this answer option, you automatically skip question 22)

22. *Checkboxes*

My ccTLD takes DNS Level Action against the following types of abuse related to trademark infringements ***in the domain name itself***. Please select all that apply.

- ☐ Homographs (e.g. an IDN homograph attack, with characters that look alike in different scripts)
- ☐ Typosquatting (registering domain names that are similar to legitimate ones, intending to deceive users)
- ☐ Fake webshops (offering for instance counterfeit products, no shipping, ID theft etc.)
- ☐ Cybersquatting (registering or using a domain name to profit from a trademark, corporate name, or personal name of an individual)
- ☐ Domain Kiting (repeatedly registering and deleting the same domain name within a grace period, effectively allowing the squatter to use the domain for free)
- ☐ Drop Catching (registering a domain name the moment it expires and is released to the public, often done using automated software to snatch up valuable domains before their original owners can renew them)
- ☐ We rely solely on third party complaints processes (UDRP or equivalent)
- ☐ None
- ☐ Other (Please specify)

23. *Checkboxes*

My ccTLD notifies third parties about DNS Level Action on domain names. Please select all that apply.

- ☐ Yes, we notify the registrant
- ☐ Yes, we notify the registrar
- ☐ Yes, we publish a report
- ☐ No, we do not provide notification

Please explain

24. *Multiple Choice*

My ccTLD has a procedure in place for the registrant to contest or appeal ccTLD action against a domain name for technical abuse and/or content complaints.

- ☐ Yes
- ☐ No
- ☐ Other (Please specify)

25. *Check boxes*
Does your ccTLD have publicly available documentation on DNS Abuse mitigation? Please select all that apply.
- ☐ Yes, we have publicly available documentation regarding the types of abusive content we are able and/or willing to take DNS Level Action on
- ☐ Yes, we have publicly available documentation regarding which requirements need to be met, for our ccTLD to take DNS Level Action against abusive domains
- ☐ We do have such documentation, but we do not publish it.
- ☐ None of the above

Page 4. DETECTION

26. *Check boxes*
Which free benchmarking services do you use to track abuse in your ccTLD? Please select all that apply.
- ☐ ICANN's Domain Metrica, formerly called Domain Abuse Activity Reporting (DAAR)
- ☐ NetBeacon Institute, formerly called DNS Abuse Institute
- ☐ None
- ☐ Other (Please explain)

27. *Check boxes*
Which methods does your ccTLD use, to mitigate DNS Abuse? Please select all that apply.
- ☐ Registration Policy and/or Terms and Conditions targeting DNS Abuse
- ☐ Internal best practices
- ☐ Procedures (e.g. post-registration checks on high risk phishing terms)
- ☐ Tools (e.g. DNS detection and threat intelligence feeds)
- ☐ Consumer awareness efforts
- ☐ Complaints procedures
- ☐ Other (please specify)

28. *Check boxes*
My ccTLD has a collaborative relationship for the purpose of abuse detection with: (Please select all that apply).
- ☐ National response team, e.g. CSIRT, CIRT, CERT
- ☐ Law Enforcement Agency (LEA)
- ☐ Trusted notifier, e.g. Internet Watch Foundation
- ☐ Trademark Association

- ☐ Academic and/or Research Institution
- ☐ Industry-specific Alliance, e.g. financial services
- ☐ Legal/Judiciary/Mediation/Dispute Resolution agency or body
- ☐ None of the above
- ☐ Other (please specify)

29. *Multiple choice*
My ccTLD entered into a Trusted Notifier arrangement (a formal agreement with a notifier) to address DNS Abuse.
- ☐ Yes
- ☐ No
- ☐ Not applicable: There is an exclusive local regulatory and enforcement authority to address a given form of abuse in my country or territory

Please specify.

30. *Multiple choice*
My ccTLD has mechanisms in place for members of the public to report DNS Abuse.
- ☐ Yes
- ☐ No

If you selected "yes" as an answer, please explain.

31. *Check boxes*
Does your ccTLD verify registrant data? Verification in this context refers to checking ID or company registration documents for instance. Please select all that apply.
- ☐ My ccTLD performs manual registrant data verifications
- ☐ My ccTLD performs automated registrant data verifications
- ☐ My ccTLD does not perform any registrant data verifications (by selecting this answer option, you automatically skip question 32)

32. *Check boxes*
When does your ccTLD verify registrant data? Verification in this context refers to checking ID or company registration documents for instance. Please select all that apply.
- ☐ Prior to registration
- ☐ Post registration
- ☐ Upon renewal

- ☐ Upon complaint, or other concerns being raised
- ☐ Upon screening for suspicious registrations
- ☐ Other (please specify)

33. *Comment box*
What type of information does your ccTLD validate at the time of registration? Examples may include - but are not limited to - phone numbers, postal addresses, company identifiers etc. Validation in this context means: doing some checks to ensure the information is likely to be real.

34. *Comment box*
What measures, if any, do you take to keep the domain name registration information accurate over time? Please specify.

35. *Multiple choice*
My ccTLD uses DNS Abuse feeds and/or threat intelligence sources.
- ☐ Yes
- ☐ No (by selecting this answer option, you automatically skip question 36)
- ☐ Not sure

36. *Check boxes*
The DNS Abuse feeds and/or threat intelligence sources my ccTLD relies on are:
- ☐ Open Source, or Community Feeds
- ☐ Commercial
- ☐
- ☐ National CSIRT or cybersecurity center
- ☐ Other, please specify

37. *Check boxes*
Which DNS Abuse feeds and/or threat intelligence sources does your ccTLD use? Please select all that apply.
- ☐ Abusix
- ☐ APWG (Anti-Phishing Working Group)
- ☐ Cymru

- ☐ DGArchive
- ☐ Forum of Incident Response Security Teams (FIRST)
- ☐ M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group)
- ☐ Netcraft
- ☐ RecordedFuture
- ☐ Shadowserver
- ☐ Sophos
- ☐ Spamhaus
- ☐ SURBL
- ☐ Other (please specify)

38. *Check boxes*
    My ccTLD uses Artificial Intelligence and/or machine learning for DNS Abuse detection and/or Intelligence:
    - ☐ Yes
    - ☐ No
    - ☐ Not currently, but planning to
    - ☐ Not sure

Please explain.

39. *Comment box*
    If you are using DNS Abuse feeds and/or threat intelligence sources, which ones do you benefit most from and why?

Page 5. MISCELLANEOUS

40. *Multiple choice*
    Post DNS Level Action, my ccTLD continues to monitor the domain for a specific period of time to detect possible recurrence of DNS Abuse.
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

Please explain

41. *Multiple choice*
    My ccTLD has DNS abuse educational materials and/or carries out outreach programs to Registrars and/or Registrants.
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

Please explain

42. *Comment box*
    Overall, what are the challenges you encounter - or encountered in the past - related to the implementation of DNS Abuse Mitigation? Please specify.

43. *Comment box*
    Any final comments? Anything we forgot to ask?