
ICANN
80
POLICY
FORUM

Virtual Participants

1

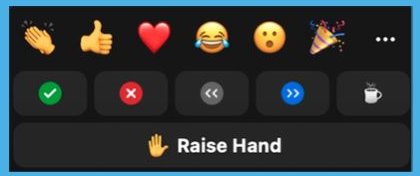
Connect your **Zoom Audio** to listen to the meeting.

2

Turn on your **Zoom Video** to be seen by other participants.

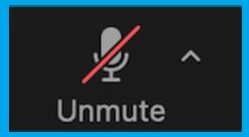
3

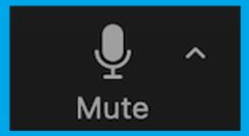
Raise your hand in **Zoom Reactions** to join the speaking queue.



4

Unmute your **Zoom Audio** when called upon to speak.

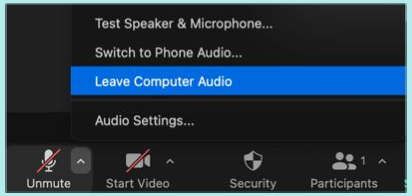




On-Site/In-Room Participants

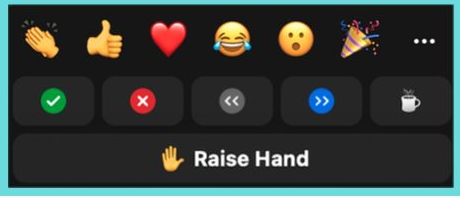
1

Do **not** connect your **Zoom Audio**. To disconnect your audio, click on the **Up Arrow** and select **Leave Computer Audio**.



2

Raise your hand in **Zoom Reactions** to join the speaking queue.



3

Use the physical microphone at your seat or in the aisle when called upon to speak.

ccNSO Members Meeting - Day 1

gTLD Base RA and RAA Amendments: what do ccTLDs need to know?

ICANN | ccNSO

Country Code Names Supporting Organization

Scene setting

ccTLDs have one tenth the level of malicious registrations seen in gTLDs*
Standards in gTLDs are set to be raised by new contract clause in the gTLD registry operator contracts and the ICANN registrar accreditation agreement
We know that abuse does not go away - it moves onto the next target - so might ccTLDs be a target in future?
What's going on in gTLD world, and what do ccTLDs need to learn?

Whether we are ccTLDs or gTLDs we are all TLDs and so it is a great pleasure to welcome friends from the gTLDs Registries Stakeholder Group to the meeting
We both have a strong interest in building strong industry standards and reputation for our internet end users and promoting safety and security on the internet
Common standards and the long term health and reputation of the domain industry is in all of our interest

*Netbeacon Institute May 2024 report

gTLD Base RA and RAA Amendments: what do ccTLDs need to know?

Tuesday, 11 June 2024 | 13:45-15:00 (11:45-13:00 UTC)

What is the impact of the amendments to the ICANN 2013 Registrar Accreditation Agreement (RAA)? What could ccTLDs learn from it?

Session chair: Nick Wenban-Smith, .uk

- Abuse amendments to ICANN RAA: Samantha Demetriou, Verisign
- Registrar perspectives:
  James Bladel, GoDaddy and Adeola Raji, Upperlink Limited
- Regulator perspectives: Babagana Digima, Nigerian Communications Commission (NCC)
- Panel discussion by Barrack Otieno, AfTLD






ICANN | ccNSO

About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

Useful resources for ccTLDs

assist ccTLD Managers to detect and/or mitigate DNS Abuse incidents

Heads up: **second survey** coming soon!

Resource library

- Presentations and reports
- Tools
- Definitions, policies
- Articles, commentaries

Geared at ccTLDs, vetted by the DASC editorial board

- Consult

https://community.icann.org/x/Ege7Cg

- Propose additional content

https://community.icann.org/x/DoWZDg

Dedicated email and contact list

- Subscribe up to 4 contacts per ccTLD
- Quarterly contact list summary
- Closed, but not confidential
- Subscription requests: require authentication

- Share information

DASC-mailing-contacts@icann.org

- Subscribe

DASC-mailing-contacts-subscribe@icann.org

- Read more

https://community.icann.org/x/BJJME

About the DNS Abuse Amendments

- Amendments to the Registrar Accreditation Agreement (RAA) and Base Registry Agreement (RA)
  - Applicable to all ICANN-accredited registrars and gTLD registries that operate on the Base RA

- The amendments establish a concrete definition of DNS Abuse:

  "Malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for the other forms of DNS Abuse listed)"

Background

Problem

Lack of a clear and enforceable obligation in the RAA and RA to mitigate or disrupt DNS Abuse

Approach

Why contract amendments?

- Ability to take immediate action to address gap in contracts
- Goal to establish a foundation on which to build with further input from the community

Impact to Registries

- Registries must **promptly** take **appropriate** action to mitigate DNS Abuse when they receive a report with **actionable evidence**

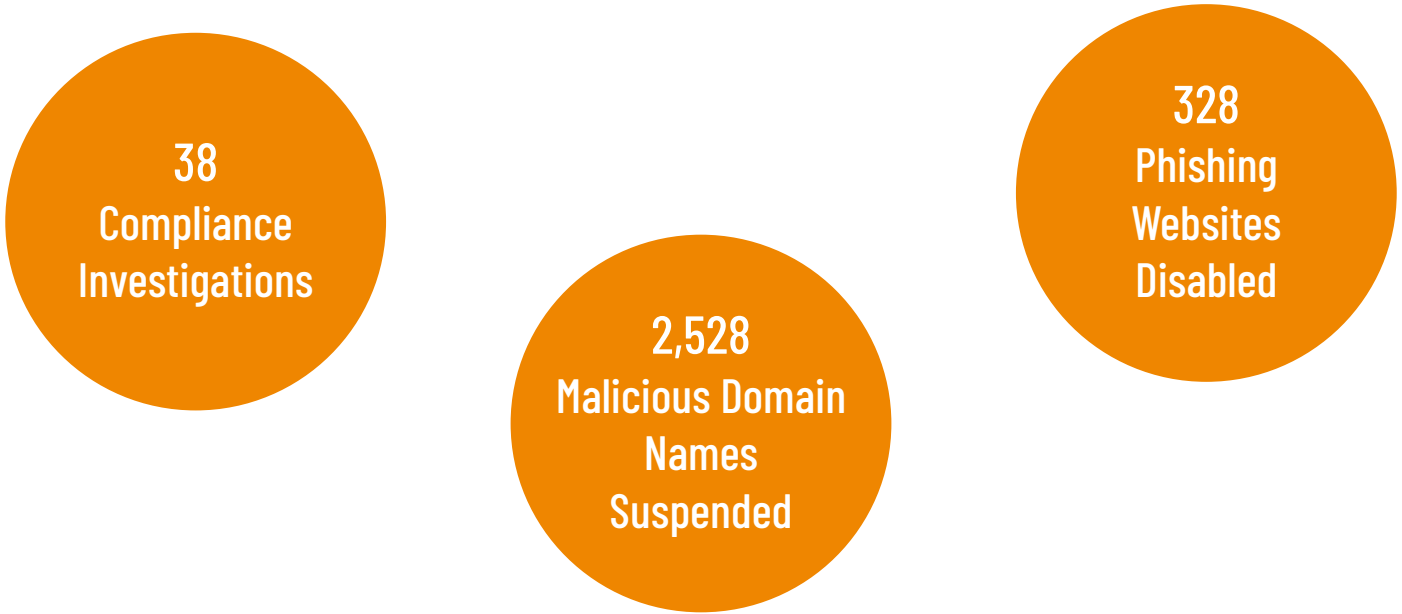
- **Appropriate action** includes referring the domain name(s) to the sponsoring registrar

- Registry may receive DNS Abuse reports via email or a webform, and must confirm receipt

Reference: Specification 6, Section 4 of the Base RA

Next Steps: Measuring Impact of the Amendments

Since 5 April 2024:



DNS Abuse Amendments – gTLD Registrar Perspectives

James Bladel - GoDaddy
Vice President, Gov't & Industry Affairs.

DNS Abuse – RAA Amendments

- Why would Registrars voluntarily agree to new contract obligations?
  - DNS Abuse is an industry-wide problem
  - Some registrars made significant investments in detection & mitigation tools
  - Commitment to self-regulation (e.g. The Framework on DNS Abuse)
- Need for standardized terminology and definitions
  - DNS Abuse: Phishing, Pharming, Malware Distribution, Botnet C&C, and sometimes Spam

DNS Abuse – Amendments Summarized

- Registrars now have an obligation to **investigate** and, if detected, **disrupt** DNS Abuse reported on their platform
- ICANN is now empowered to investigate and sanction Registrars who are not making a sincere effort to comply with the amendments.
- The Amendments do not cover other categories of abuse, such as content or IP infringement

DNS Abuse – The Story So Far (Registrars)

- The new Amendments took effect on 5 APR 2024
- For many Registrars, the new rules did not require significant changes to their existing practices.
  - Previous compliance efforts (e.g. DNS Framework) were already aligned.
- There was (is?) some concern about a significant increase in the volume of reports

DNS Abuse – The Story So Far (Industry)

- exDNSAI– Now NetBeacon is providing Registrars and Registries with reports and performance metrics.
- These have clearly identified which contracted parties are embracing the new rules, and which need additional outreach/education/coaching.
- NetBeacon data also demonstrates different categories of abuse, e.g. New vs. Compromised domain registrations.

DNS Abuse – The Story So Far (ICANN)

- ICANN is now receiving reports of DNS Abuse violations
- Volume is up, but some are being rejected.
  - For example, simultaneous submission to ICANN and the Registrar
  - Or incomplete/insufficient report data.
- ICANN is also focusing on systemic failures, vs. single incidents. (for now)

DNS Abuse – Suggestions for ccTLDs

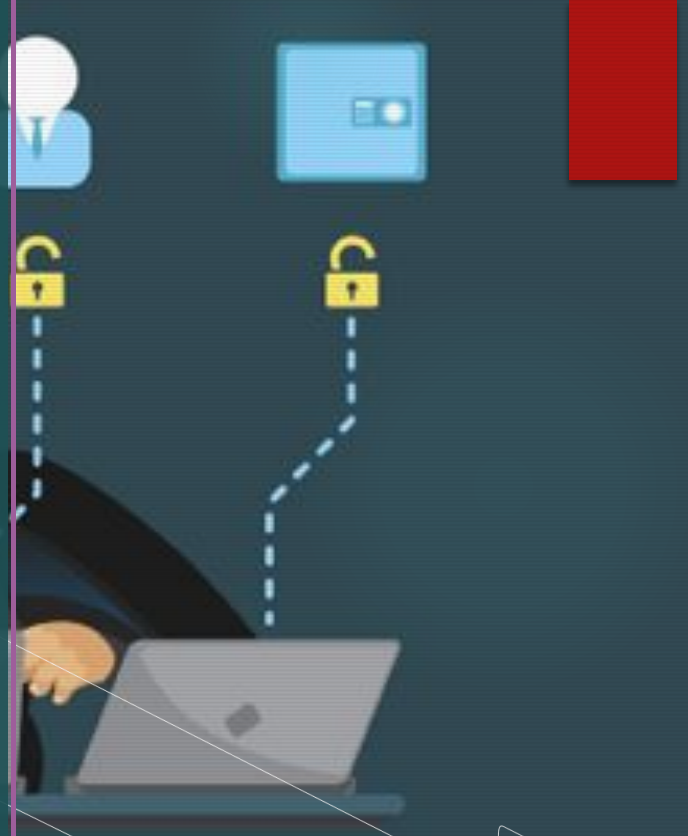
- Standardization – Don't reinvent the wheel
  - Align new DNS Abuse policies with the gTLD contracts.
  - Model terminology & definitions with adopted standards.
- Trust registrar decisions
  - Overly prescriptive policies only aids the threat actors.
  - Registrars, esp. global providers, have experience and expertise
- Join a united industry effort against the problem of DNS Abuse

Thank you!

Q & A

DNS ABUSE AMENDMENT

Adeola Raji
(Domain Manager, Upperlink Limited)



busive use of the dom nain name system and website content

Outline

- Understanding DNS abuse amendment.
- Why this Discussion Matters?
- Agenda Overview
- a. What is the impact of DNS abuse on registrar businesses?
- b. The challenges of operating at scale in multiple jurisdictions and TLDs.
- c. How CCTLD can help to fight abuse
- Conclusion

Understanding DNS Abuse Amendments

2013 Amendments

- Establish abuse reporting contacts.
- Review abuse reports within 24 hours. However, they did not mandate specific actions after the review

2023 Amendments

- Registrars must take prompt and appropriate action on actionable DNS abuse reports.
- DNS abuse is clearly defined, including malware, botnets, phishing, pharming, and spam used for these purposes.
- Abuse reporting mechanisms must be easily accessible, with confirmation of receipt.
- Enhanced cooperation with law enforcement is emphasized.
- Proactive monitoring and prevention of DNS abuse is encouraged.

These updates aim to strengthen the response to DNS abuse and enhance internet security.

Why This Discussion Matters

These changes aim to combat the increasing instances of DNS abuse, such as phishing, malware distribution, and botnets, which threaten the stability of the internet.

Today's presentation will cover:

- The impact of these DNS amendments on registrar businesses.
- The challenges of operating at scale in multiple jurisdictions and Top-Level Domains (TLDs).
- How country code Top-Level Domains (ccTLDs) can help fight DNS abuse.

These amendments bring enhanced tracking and accountability, stricter compliance requirements, and increased transparency. We will explore what these changes mean for registrars and how they can adapt to these new requirements. Additionally, we will discuss the operational complexities in different jurisdictions and the vital role ccTLDs play in mitigating DNS abuse. Let's dive in.

Impact of DNS Abuse Amendment on Registrar Businesses

- Tracking and Accountability
- Improve Complainant Accessibility
- Protection for SMEs
- Collaboration Among stakeholders
- Reduce Legal Conflicts

In essence, new DNS modifications will improve registrar tracking and accountability, making it easier to comply with ICANN requests, increasing reporter access, and reducing legal issues. By adhering to all of the registrar requirements in the revised amendments, registrars may effectively manage these changes and benefit from enhanced trust and stability in the domain registration ecosystem.

Challenges of Operating at Scale in Multiple Jurisdictions and TLDs.

- Keeping up with different rules in different jurisdictions could be exhausting
- Navigating various TLD Practices.
- Ensuring data security.
- Building capacity to accommodate future challenges.

The new DNS abuse amendment complicates operating at scale across multiple nations and TLDs. It requires firms to navigate complex regulations, cultural differences, and technological systems to maintain a safe and trustworthy online environment.

How CCTLD Can Help Combat DNS Abuse?

Country Code Top-Level Domains (ccTLDs) play a crucial role in combating DNS abuse, and they can significantly enhance these efforts by ensuring that the public are well-informed about their rights and the actions to take when facing challenges. Here's how ccTLDs can help fight DNS abuse and the importance of awareness:

- Clear rule
- Checking Registrations
- Easy Reporting
- Educating registrants and law enforcement agencies about DNS abuse and best practices for prevention and reporting.
- Collaborating with law enforcement agencies to detect, investigate, and prevent DNS abuse effectively.
- Working with registrars to ensure everyone follow rules.

Conclusion

Country code Top-Level Domains (ccTLDs) play a crucial role in combating DNS abuse through localized monitoring and enforcement. Their proximity to local issues allows for quick response and collaboration with local authorities. Additionally, ccTLDs can help educate registrants on their rights and responsibilities, raising awareness and promoting proactive measures against DNS abuse.

THANK YOU

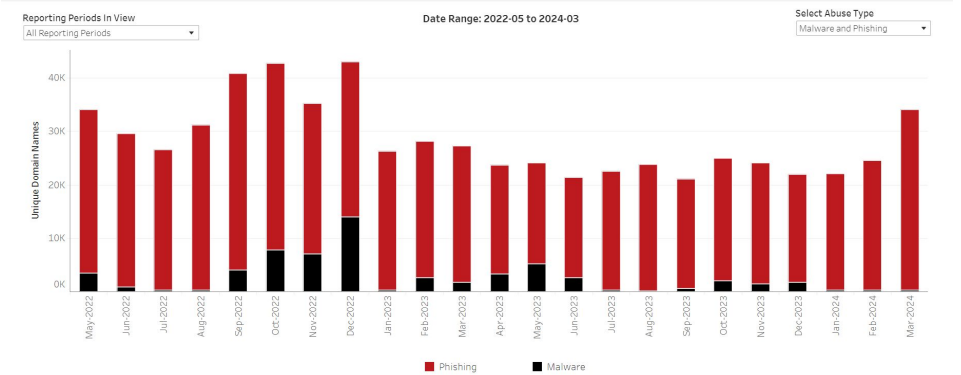
gTLD Base RA and RAA Amendments: what do ccTLDs need to know?
- A Regulators Perspective

Engr Babagana Digima
Head New Media & Information Security Department
Nigerian Communications Commission (NCC)

ICANN | ccNSO

Background and Context

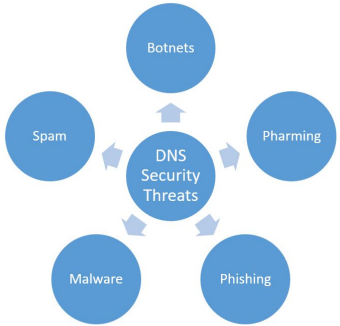
- ICANN's recent amendments to gTLD registrar accreditation agreements introduce enhanced measures aimed at mitigating DNS abuse.
- These amendments are critical for ccTLD managers as they establish a global baseline for anti-abuse efforts which are directly applicable or serve as a guideline for ccTLD operations.
- The recent amendments by ICANN towards a more secure and abuse-resistant internet, signify a need for regulatory alignment and proactive engagement.

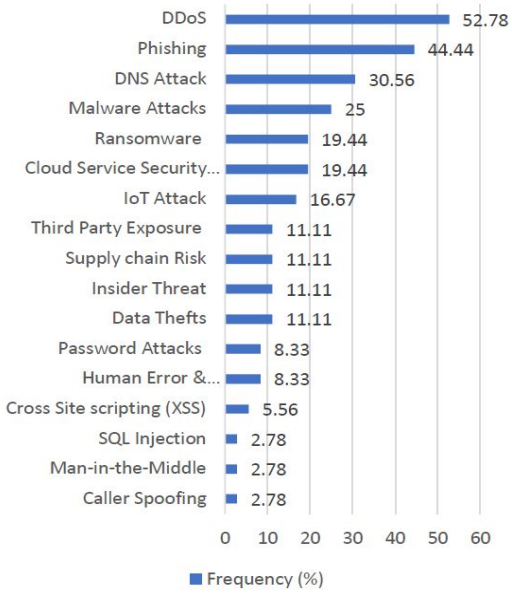


Aggregate Trends- Phishing and Malware (Netbeacon Institute, 2024)

The Impact on Nigerian Citizens

- **Improved Online Safety:** The implementation of these amendments is expected to significantly reduce instances of online abuse, phishing scams, and malware, directly enhancing the safety of Nigerian internet users.
- **Strengthened Infrastructure:** The .ng ccTLD will benefit from enhanced measures against abusive registrations, thus protecting our national brand in the digital space.
- **Support for Local Businesses:** Local businesses that rely on the .ng domain for their operations will enjoy a reputation as safe and secure, attracting more customers who feel confident in their online interactions.





Cyberthreats in the Communications Sector
(Annual Cybercrime Index, Intelligence and Threat Landscape NCC, 2024)

Challenges for Regulators and ccTLD Managers

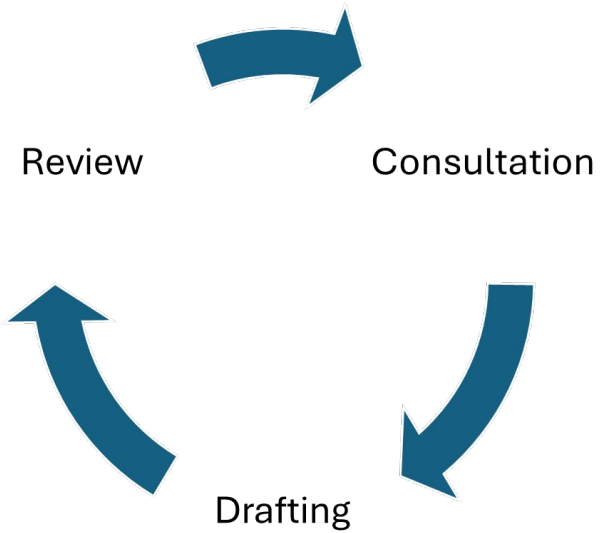
- While these amendments are a step towards a secure digital ecosystem, their implementation poses challenges including awareness, regulatory alignment, capacity building, and technological adaptation.

- For ccTLD managers, the necessity to balance international standards with local realities is paramount

Role of Regulators in Facilitating Compliance

- Regulators can act as catalysts for change by drafting supportive policies and regulations, encouraging stakeholder dialogue, and facilitating technical assistance.

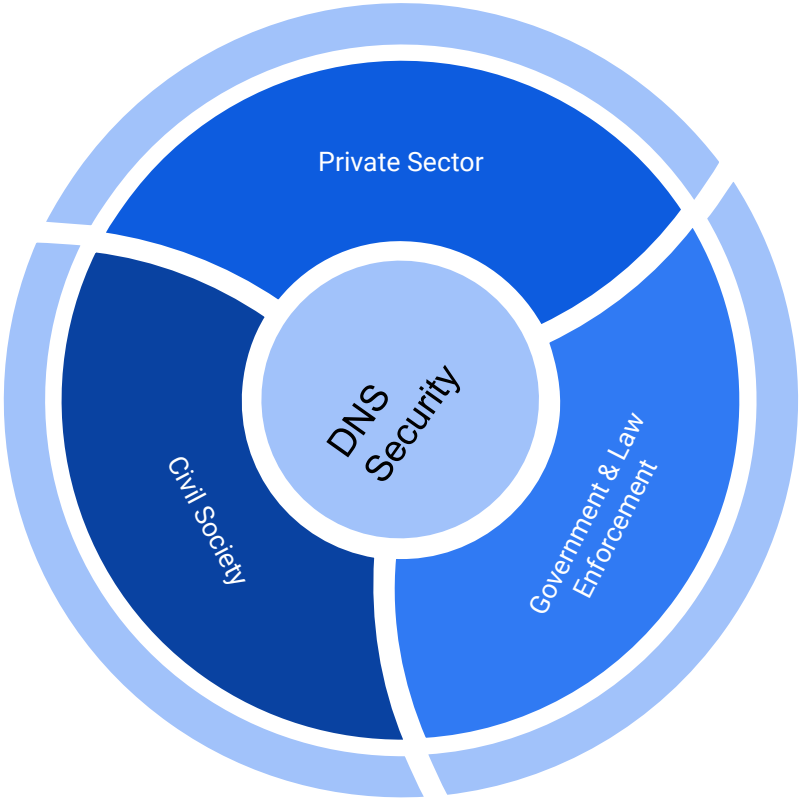
- By aligning national policies with ICANN's standards, we not only enhance our ccTLD's reputation but also protect our digital borders against abuse.



Policy and Regulations Development Process

Collaborating with other stakeholders

Effective DNS abuse mitigation is not a solo journey but a collaborative endeavor. Engaging with a diverse array of stakeholders - from government and law enforcement to the private sector and civil society - enriches our strategy, ensuring a holistic and inclusive approach to securing the digital ecosystem



Future Directions and Strategic Initiatives: NCC's Measures

- **Comprehensive Review**
  - The NCC is undertaking a review of the amendments to assess their implications and to develop a comprehensive adaptation plan.
- **Policy Alignment**
  - We are aligning our policies and regulatory frameworks with the amendments to ensure a cohesive approach to DNS abuse mitigation.
- **Stakeholder Engagement**
  - Engaging with stakeholders, including Nigeria Internet Registration Association (NiRA), ISPs, domain registrars, and the general public, to ensure a collaborative approach in the implementation and enforcement of these amendments.

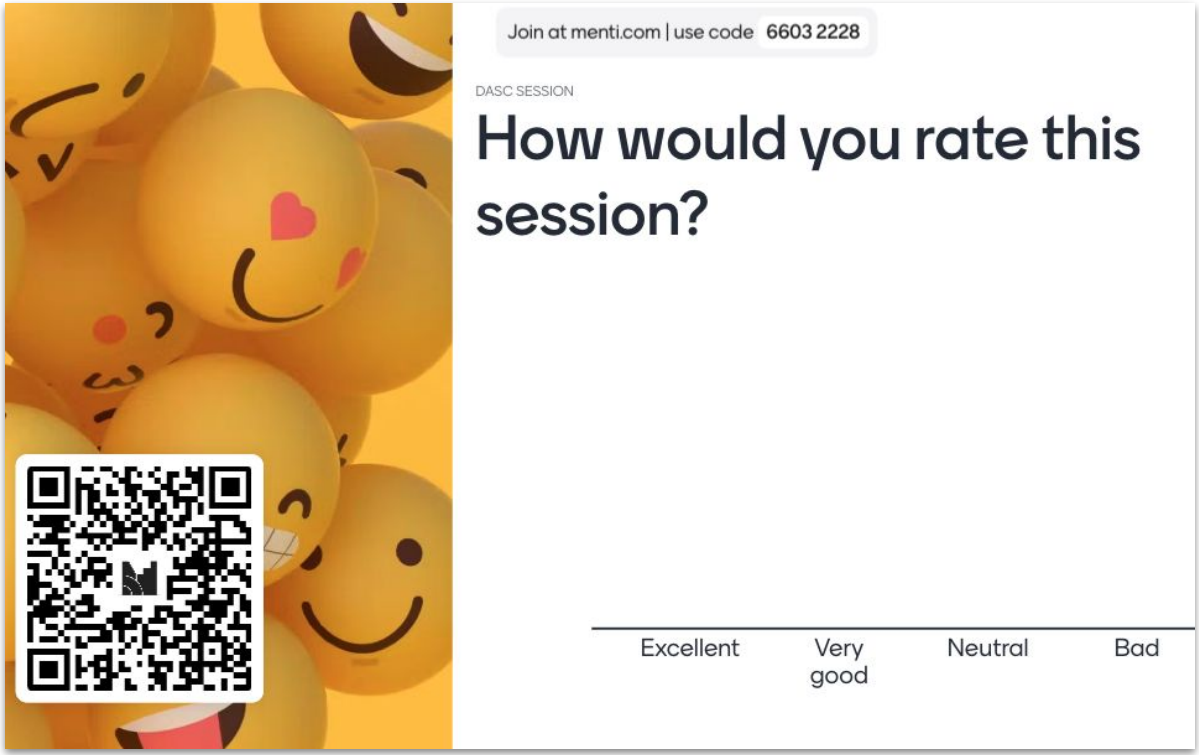
- *Looking ahead, we plan to adopt advanced technological tools for real-time abuse monitoring, enhance our frameworks to include specific provisions against DNS abuse, and foster international cooperation.*
- *Our aim is not just to react to abuse but to anticipate and prevent it.*

Conclusion and Commitment to Safer Internet

In conclusion, the journey towards a safer internet is ongoing and collective.

As regulators, we are committed to adopting, advocating for, and adapting to these global standards, safeguarding the .ng domain, and ensuring it stands as a beacon of trust and security in the digital world.

Thank you!



Coming next:

ccNSO Universal Acceptance Session, tomorrow at 7 UTC (9 am local time)