ICANN82 | CF – ccNSO: DNS Abuse Standing Committee Session
Wednesday, March 12, 2025 – 13:15 to 14:30 PST

CLAUDIA RUIZ

Hello and welcome to ccNSO DNS Abuse Standing Committee session. My name is Claudia Ruiz, and I, along with my colleague, Susie Johnson, are the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom.

When called upon, virtual participants will be given permission to unmute in Zoom and on-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation. Thank you. And with that, I will now hand the floor over to Nick Wenban-Smith, Chair of the session. Thank you.

NICK WENBAN-SMITH

So, this topic was selected, actually quite a clear winner in our whole of options at the Istanbul ICANN81 meeting. And on

Saturday, just to give you a heads up, the two topics which have come up top of the list for future working is going to involve Artificial Intelligence in the role of combating DNS Abuse.

And Artificial Intelligence was definitely the winner. And also, a slightly different topic, which would be a dedicated Deep Dive workshop looking at financial crime on the Internet and scams and the role of malicious registration of domain names in facilitating those financial crimes. So, that's how we got to and that's roughly what is going to come up in the next couple of ICANN meetings. So, we've got a slightly different format today with a bit more informality. Before we start, I would like to thank our host country, U.S. dotUS. And I've got Fernando just to give us a little bit of a promo following on from the excellent ccNSO social last night.

FERNANDO ESPANA: Well, good afternoon, everybody. My name is Fernando Espana from dotUS. And first of all, I hope you all had a good time last night. Those of you who attended the networking event, we appreciate your attendance. And I think I saw a lot of happy faces last night. And I know lunch, the sessions after lunch are a little bit tough. So, we have some cookies in the back for you to get some energy. So, please feel free. And I know it's already on the fifth day of the meeting, but welcome to Seattle. Thank you. Enjoy.

NICK WENBAN-SMITH: Now, it's a big thank you to our friends at GoDaddy Registry for the US reception and sponsorship of the meeting. This interesting

topic of registration data and the intersection between collection of registration data and verification of registration data, and how this intersects with prevention of DNS Abuse and mitigation of DNS Abuse. It's quite a complicated topic.

So, I'm very pleased to have, first of all, two presentations from two different ccTLDs. I've got Bob from .NZ. Thank you, Nigel. And Kristian from .se. So, there's a geographically diverse selection of speakers. I'm just talking about what those ccTLDs do in terms of collection and verification of registration data, and how it impacts on their efforts to combat DNS Abuse. And then I think we want to have a bit more of a Holistic View. One of the important things in the terms of reference for the ccNSO DNS Abuse standing committee, one of the key things is outreach to different parts of the ICANN community.

So, I'm very pleased to have my good friend, Reg, who works for Tucows. Tucows is obviously a global registrar. And they have a different perspective in the sense that what they deal with is not just an individual ccTLD and its policies, but multiple different ccTLDs with multiple different policies, and then all the gTLDs. So, how does that all work? And are there better ways to do this collectively?

And then Chris Lewis-Evans, who is not here in his commercial promotion role, but is sort of from the perspective of a former officer in the UK National Crime Agency, talking about it from law enforcement perspectives. And I apologize, by the way, there's a bit of misinformation on the slide around the timing of the session.

It is not Tuesday at 10:30. Just in case you had thought that this was some sort of Kafka simulation in a multiverse alternate reality.

So, I'll hand over first to Bob and then to Kristian. If you've got any thoughts or comments, this is supposed to be a less scripted, more interactive thing. That's why we're not behind the desks. I'm going to walk around. And like I said in my session on Saturday, you have to speak something. So, if I was you, I would say something interesting early on, because otherwise you might get picked on and all the easy stuff to say would have been taken up.

So, just plant that there. I am going to pick on people to say things. So, be volunteer ready. Thank you. Over to Bob. Oh, we've got some more slides. All right. So, this is a standard set of introductory slides. This is just to remind attendees. By the way, is anyone here at their first ever ICANN meeting? Excellent. Thank you and welcome. So, it's a very nice group and it's a very safe place. So, I'm really interested in how you find the meeting. So, at the end of it, I might ask one or two of you to let us know how you find it, if that's okay.

And actually, who can my fellow members of the DNS booth standing committee, can you identify yourselves through a visual show? Thank you. So, Fernando, Bruce, Olga, Chris, and David. Thank you all very much. And Bob. So, as an important reminder, we're not here to formulate policy. We are here to share information, best practices, learn from other people's ideas and mistakes, promote an open and constructive dialogue, and

fundamentally, we do want to push down DNS Abuse across all the ccTLD ecosystem.

And we understand that a ccTLD is just a TLD, and there's no point moving abuse from one ccTLD to another ccTLD. We'd rather eliminate it. And also, although it's good fun to see how little abuse there is in the ccTLD community versus the gTLDs, it is important for our citizens that we push down the levels of abuse across the whole ecosystem, including gTLDs. So, next slide. So, we have just here a list of the resources. There's an abuse library.

There's a dedicated email and contact list for people who want to participate and to get more messages directly. We've done two global surveys of the ccTLDs, one in 2022, one in 2024. The findings of those surveys are in the records as recordings. So, if you're interested, go and have a look at those. And we've held workshop sessions on understanding levels of abuse in your ccTLD through the tools and measurements workshop. There's lots of free resources provided to all ccTLDs. If you are not sure how much abuse you have in your ccTLD, then there's no excuse, really, because there's plenty of excellent free resources available, however large or small you are as a ccTLD.

We also talked about emerging standards in terms of the contractual provisions in the ICANN regulated gTLD space in terms of obligations on registries and registrars to action reports of DNS Abuse and how that was going on and maybe some ccTLDs adopting equivalent provisions. So, in the context of coming into the real topic here of registration data. In the 2024 survey, and this

is the good sort of introduction, this is already an introduction to the topic today.

You'll see that there's a lot of different practices in terms of verification of registrant data, including none. So, some people don't do any registration data verification. Some people do a lot, and the sorts of registration verification that they do depends a bit on the model of the registry manager.

So, you can see there's manual registrations, there's automated, there's no registrations only upon a complaint being received or another flag for suspicious activity, sometimes on renewal, sometimes on transfer, sometimes before registration, sometimes after registration. So, there's a variety of different things across the landscape.

Next slide. Okay, so I'll give you a little moment to do the Menti.com. Okay, is everybody logged in who wants to? Or does anyone need a bit more time? I'll just do it myself.

Okay, so just to get a bit of a temperature in the room. How much do you agree or disagree with the statement about accurate registration data is useful as a tool to combat DNS Abuse? Still numbers ticking up, 35 responses, 37, 38, 39, 40, 41. You can see the numbers settled. There're more votes coming in. But basically, it's settled around the 8.4, 8.5, 8.2. Roelof, you just asked a question. Do you want a second question? Roelof, have a second question.

ROELOF MEIJER

Well, maybe it's more of a statement. Roelof Meijer from .nl for the record. It depends a bit, I think, how you read this phrase, because I think accurate registration data is a good tool to prevent abuse. I'm not sure if it's a good tool to combat abuse, because most of the time bad actors won't submit their accurate registrant data. Do you get what I mean?

NICK WENBAN-SMITH

I get what you mean. I get what you mean. It's interesting that you've, because I think when we've done several of these Mentimeter polls, I've looked at the question and thought, oh, depending exactly how precisely you read it, you might get different answers. So, I think an ambiguity in the question is not helpful. The reason why it's expressed quite a general to combat, because some, as we get into this, some ccTLDs will use a complaint about a domain name for criminal purposes, and they will use the verification of registrant data as the method to take the domain name out of the DNS.

So, that's why it's a mitigation thing as well as a prevention thing. Sorry, Nigel, you've got your hand up as well. I think this is why it's a very interesting question. It's quite a nuanced topic. And I think this is part of what we want to get out of this session, is that it's a lot more complicated than you might think.

NIGEL ROBERTS

Yeah, thank you. I'm just going to add a little coda to what Roelof said, whom I agree with. But we are one of those ccTLDs that you

mentioned a minute ago, Nick. And I would phrase it completely differently, which is why I strongly disagree with the question. Inaccurate registration data is useful as a tool to combat DNS Abuse because we get contacted about some real or maybe imagined complaint about a domain name.

The very first thing we do is check the registration data. If the registration data looks at all slightly inky, to borrow a West Coast phrase, we put it into verification. And if we don't get verification within a reasonable period of time, we suspend. And usually, it just stays there suspended for eternity.

NICK WENBAN-SMITH: Hold those thoughts. Are there any more preliminary comments around the question before we get into the presentations? Okay, let's get into presentations and hold those thoughts because I think it'll feed into some of the things you're about to be talked about and to discuss. Okay, but it's still 8.1 out of 10, pretty high.

BARBARA PEARSE: Hello, everyone. I'm Barbara Pearse from the Domain Name Commission. I'm the commissioner there and I'm just going to give you an overview of how we manage data validation and ID verification in the .nz ccTLD. Next slide, please. So, just to give you a little bit of an overview of what our rules or policies say in respect of the eligibility criteria to register a .nz domain name, you need to be an identifiable individual over 18 or a lawfully constituted entity.

.nz does not have any local presence requirements, so that can sometimes make it difficult to try and identify individuals in other jurisdictions. The other method we use is the registration data must be accurate, complete and kept up to date. We collect quite a lot of information, including the registrant's name, address, city, postcode, country, as I've listed there.

And as the gentleman over there said, we also will be able to suspend or cancel a domain name if determined the data is incorrect or the identity is not verified within the requested timeframe. So, we've got two methods of doing this. We've just recently had established an automated tool to read flag suspected malicious domain names. It will assign a threat level score based generally on the domain name itself and the registration data information.

The team will then manually sense check the initial threat level score to see if any other potentially harmful domain names haven't got the highest score. Examples of that would be if they have references to government or immigration or financial services like banks in the name, then we'll up the threat score and we will put those through our data validation process. So, that's a manual process where we send out a request for the domain name holder to respond to us and confirm the details.

The other method is reactive sample, which is people, members of the public or agencies referring suspicious domain names to us. And then we will put that through our data validation process as well. In respect of identity verification, we have biometric testing,

which is the best method that we've come up with, particularly with the multi jurisdictions. And that requires the domain name holder to take a selfie with their identity photo identification to pass that test.

What we find is often if the first step we'll take is the data validation, if that's validated and we feel it's still suspicious, we'll put them through the identity verification process. Often what we see happening is the links to undertake the biometric testing are not activated and so they don't engage in the process and so we will suspend the domain name.

NICK WENBAN-SMITH And the domain name remains live until?

BARBARA PEARSE Yes, so all our testing is done post registration and it's in the zone. So, there's no hold until the validation process is completed. This is just an example of some of the stats that we've gathered just on the first three-month sample. In respect of our tool, the proactive numbers, we had 226 come in. 216 did not validate the data, so we put them through our ID verification process. Seven of those didn't engage with it and three verified.

So, it's looking quite promising in respect of the suspicious names that it's identifying for us. In respect of the reactive sample, the data not validated is 51. So, we put them through the ID verification and three did not verify. So, the ones that didn't were suspended. In respect of why is the reactive sample a lot lower

	than the proactive? Often, you'll get people complaining about domain names. They could be competitors of the domain name holder or they may have issues with the content or the use of that domain name. So, it seems appropriate that a lot of those might still verify because they're legitimate domain name holders and use.
NICK WENBAN-SMITH	So, if I understood this right, essentially of the proactive sample, so these are the new registrations which look suspicious. And in fact, only three of those, so slightly over 1%, so slightly under 99% malicious by the look of it.
BARBARA PEARSE	99% were suspended, so they were malicious. Three were legit.
NICK WENBAN-SMITH	Whereas out of the reactive sample, more of those guys go through to verification because they're presumably potentially older domain names.
BARBARA PEARSE	Or they could be compromised.
NICK WENBAN-SMITH	Or they could be compromised, exactly.

REG LEVY Right, so with the proactive, you had 226 total and a total of 226 either verified or suspended. But with the reactive, you have 97 total. And I'm a lawyer, so my math isn't great, but it looks like it's just over 70. So, I'm wondering what happened to the other 20. 54 and 21. Are 97? Okay, then ignore me.

BARBARA PEARSE But yeah, the proactive tolls.

REG LEVY Correct. On the proactive, they're fine. But suspended is 54 plus 21, you're going to make me do this live, is 72 domains.

NICK WENBAN-SMITH This is a very stressful experience. I'm not even doing the numbers.

REG LEVY And he told me they were right, and I was like, okay.

NICK WENBAN-SMITH So, I will say I did do first year maths at Cambridge University, but that was more complicated, and I'm not very good at arithmetic. But I don't think that 51 plus 3 plus 21 adds up to 97, isn't that your point?

REG LEVY Right, so I'm just wondering where the domains, like where we lost 20 domains.

BARBARA PEARSE It's probably just a calculation error. Okay, thank you. Overall, the reactive ones verify and validate more often, yeah.

REG LEVY Right, so I was hoping that they might actually end up in the green column, because then it would be about 50-50. But if they end up in the red column, then that's closer to 25% are bad, which is also, both of those numbers are useful numbers. Yeah, thank you.

BARBARA PEARSE And so overall, we've got approximately 750,000 domains in our space, so it's less than 1% overall that are in the abuse space. Next slide, please. So, I guess we would be of the view that we do see a strong correlation between inaccurate data leading to being an indicator of abuse. And that's the predominant tool that we have in .nz, we don't consider use or content.

In respect of the categories that we are finding, our biggest one is fake web shops or brand impersonation, followed by phishing, followed by fraudulent impersonating government, immigration, financial institutions, banks, lotto agencies, gambling. So, that's what we're mainly seeing. In addition to the compromised, and in respect of the data for domain name holders, when they're compromised, I think it's useful that it is accurate and correct and

up to date, because then they're contactable, often by our national cybersecurity agency to help them fix the issues. So, that's all I had, and if there's any more questions.

NICK WENBAN-SMITH

I think I've got a number of questions around essentially the public policy elements of, it's a small number like 1%, which seems to be maliciously registered. The verification process is obviously an effort for the registry in terms of overhead and costs, it's also inconvenient in terms of the user experience if you're a domain name registrant. So, there's obviously a sort of a balance between trying to keep the TLD safe, and to let people go about their lawful business. So, in your view, you got it about right, in the sense that it's 1%, you're not heavy handed with it, and you try to sort of not make it too poor an experience for the person, the vast majority of your legitimate registrants.

BARBARA PEARSE

Yeah, I think that's correct. And also, because resourcing and capacity and the other things you need to do, we take a risk-based approach, hence why we do the sample and just go for the higher ones. Yes.

KRISTIAN ØRMEN

Next slide please. And next slide again. So, my name is Kristian Ørmen, I'm from INTERNET STIFTELSEN, Swedish Internet Foundation, and we are the registry for .se and we also administer .nu. Next slide please. So, I have just a couple of quick stats. We

have around 105 registrars, we are open to registrations from all over the world.

We do have quite strict registrar requirements, and we also have requirements that the registrar needs to verify the registrant. But I would add to that that we are trying to be reasonable about it. We have almost 1.7 million domains in total, and we have a pricing model where we have different incentives to registrars, and that's also why I added our average registration price.

One of the incentives is that we give a discount to registrars that use eID to verify the registrants. That's great for some of our registrars, but not all. Next slide please. So, first, will registrant verification fix abuse? No, absolutely not. Yeah, inaccurate data is a great tool to close down abuse sites, I agree to that. But no matter how we do verification, how many domains we get verified, it's not going to fix abuse. Definitely not. Abusers will get better to get around the rules, and also, we can't do a bank-like know-your-customer verification when you sell a domain for €1 sometimes, or in our case usually a bit more expensive. But we need to be reasonable about it, and we need to look at the abuse when it happens.

And no matter if it's accurate data or not, there will happen abuse, and we have to deal with that somehow. Like I added on my slide, of course it's helpful for the police if we can provide accurate registrant data when they come. And I don't really like when they contact us and we're like, yeah, this domain is registered to Donald Duck. That's not a great feeling. But on the other hand, the

alternative sometimes is that this is registered to company AB, but that data was also wrong because it was just taken directly out of the company database when it was registered.

So, again, even though it's good data, it's then invalid since it's not the registrar. And of course, in the case of websites that have just been misused or hacked or something, of course good data is good, so we can contact the registrant. Another thing that is very important to me and my registry is that we want correct data on the domains because we want to make sure that the registrants don't lose their domains.

We want to be able to verify a registrant when they come and say, like, I lost my domain and this registrar and the registrar won't help me. And then we look and again, Donald Duck, and we would be like, but no, it's not your domain. Like, if your name is Anders Andersen, it should be Anders Andersen in the registrant data and then we can help you because then we can verify that you own the domain. That for me is probably the most important to why I want correct registrant data.

So, I said before that we try to be reasonable about our requirements on verifications. I usually, when a registrar asks me, like, but how much should I verify? How accurate should it be? And I usually said, well, I at least expect not to see obvious fake data. So, if you are a registrar in Sweden and you have many, many Swedish customers, there's open data you can use to check the company if it exists and the name is correct and so on. And that's a good verification method. But if you would have to even find who

is signatory and ask them to log in and so on, that's too much. So, we don't require that from registrars. But we have implemented some new systems where we require a bit more. So, next slide, please.

So, for new domains, there's the eID discount I talked about before. But we also started with this pre-delegation verification where we look at the registration we get in. And if that check fails, we are going to have the domain and server hold and we are going to send an error to the registrar and we are going to ask them to re-verify the registrant. And there we are a bit more-strict and so you have to do an actual verification of this registrant.

So, we designed this system in a way like the most important was let's make it possible to extend the system later but without introducing any change for registrars. And that's why we did it like this. So, they get an error, they have to re-verify the registrant. But our checks we can extend over time. We can start using external data sources. We could get an AI to look at it and see if it's a bad domain or something. We can change that over time but the registrars will have the same experience and that's very important for us.

So, right now it's a new system so we on purpose are very mild about it. I think we have maybe have cached like a hundred domains in two months or something. We have checks that we haven't activated yet so we can take it up over time. But both we and the registrars need to get used to these. So, that's one of the reasons it's pretty slow.

NICK WENBAN-SMITH Sorry just when did you start the eID solution? Its recent?

KRISTIAN ØRMEN So, the eID incentive it's a discount we started that 1st of January 2023. We now have like the two largest registrars using it and a bit of the smaller. And we are now up to 40% of new registrations is eID validated.

So, that incentive 25 kroner it's around $2.5. It helps pay the cost of the systems they are using. So, for some registrars especially the big ones it's of course very interesting. They save a lot of money on their registrations.

NICK WENBAN-SMITH So, I've got a couple of questions. Luc, I think was first in the queue. I can see Bruce wants to make an intervention and then maybe Reg. No? Oh Chris.

LUC SEUFER One, two, three. Yeah, Luc from EuroDNS. I have a question for Barbara, I think. I'm sorry I did not catch your name. Maybe I'm becoming a bit too conspiracious. I see conspiracy everywhere. So, I've seen the term fake shop a lot this week on a different presentation. And I'd like to know what you mean by that. Is it someone impersonating a shop to obtain the details the payment details of the user? So, it's phishing? Or is it a shop that is selling counterfeited goods? And then it would be more within the realm

of an IP or consumer protection issue. So, I'd like to know the difference if you could expand on that.

BARBARA PEARSE: From our perspective it's more brand impersonation. So, known brands with a name tweaked and a domain name that then appear in the website to look like that organisation. It could be phishing but we don't go through an analysis to determine that or not. So, we just go through the data validation process and it usually gets suspended most of the time.

LUC SEUFER: So, not DNS abusers per the ICANN definition?

BRUCE TONKIN: I might just comment on the fake shop one. Another definition of fake shop is when you order something and nothing gets delivered. Which is increasingly what we see. So, it looks like a real shop. It's got goods and services on it. And a person pays with a credit card and their credit card gets charged. But they get no goods. Well, it's not really phishing because it's not necessarily looking like any particular brand. It's just a shop with things to buy.

NICK WENBAN-SMITH: It's very interesting because I think in our review which I discussed on Saturday. They talked about oh we should spend a bit more time on sort of the definition of some of the terms. What's abuse? What's phishing? And what I found is that you can spend a lot of

time talking about the definitions of what's partly phishing. What's partly financial crime? What's partly intellectual property infringement? And there's a lot of layers. But I think fundamentally these are criminal activities. And so most ccTLDs would penalize that and have policies and processes in place to take it out of their TLD fundamentally. But I think it's interesting. Is a fake shop phishing? It might be.

BRUCE TONKIN: And just a question for Kristian. You were mentioning eID. Do your service provider or registrars, do they get charged by the government to do a check using that system? Or is it free to them?

KRISTIAN ØRMEN: Well, there's different eID solutions and we are open for the registrar to choose the one they want. And we have set some small standard requirements. In Sweden there is a big one called Bank ID and there is a small transaction fee and it is way, way lower than our incentive. So, for them it's quite good. But if you have registrants from other countries that wouldn't work. So, you would have to find another eID provider that could solve those countries.

NICK WENBAN-SMITH: Yeah. Super interesting. And is it clear on the face of the registry lookup records like RDAP or WHOIS equivalent that the domains have been verified through something as trustworthy and secure as a genuine eID?

KRISTIAN ØRMEN Currently we don't show it in WHOIS. We only currently use it for the incentive.

NICK WENBAN-SMITH Got it. Chris? Chris Lewis-Evans.

CHRIS LEWIS-EVANS Yeah. So, Kristian, so on this slide I wonder, you said it's been running two years?

KRISTIAN ØRMEN The eID, yes.

CHRIS LEWIS-EVANS Do you have any data around the level of abuse for those that registered via this mechanism versus not verifying their eID?

KRISTIAN ØRMEN I don't have that data currently. Like last year we were only at 20%. Now we're up to 40%. The volumes are getting bigger. But I would say that the most abuse we see is also from registrars that don't use the eID incentive. So, I don't think there would be a big change. But we haven't like deep dived into that numbers yet.

NICK WENBAN-SMITH Are you going to turn the screws on registrars who don't? Are you just using the financial? You're using the carrots. Are you going to let the clients stick? Or are you just going to leave the financial incentive to do its work?

KRISTIAN ØRMEN Well, for eID we just give this incentive. When we come to abuse, we have very mild requirements on registrars in our contract today. What we do have like made more intense on registrar is on the verification part. And on like all domains. Last year I don't remember if I put that on next slide. But we can go to next slide and we can see. But we put in a requirement on our contract on registrars that if they are aware of incorrect data in the registration, they must act on it.

Contact their customer and if it's not changed within a reasonable time, they must deactivate the domain. So, that's one of the things we added on registrars which is a huge burden considering that there are many old domains with incorrect data. But it's also good in a way that for example if you see abuse domain like I think all of us know that quite often it has incorrect data. Not always but quite often.

REG LEVY A question about the eID with the incentives to the eID. It sounds like it's very easy to verify somebody in Sweden through the eID method. But it might not be to verify somebody in the UK in the same way. So, can a registrar get the preferred pricing for the

domains that they do provide eID verification for but not have the incentive for the domains that they don't. Or is it a blanket yes or no.

KRISTIAN ØRMEN Per domain.

REG LEVY Interesting. Thank you.

KRISTIAN ØRMEN So, we have an extension. The registrar has to show if they use the eID or not. And then we have as one of our questions in the audit that if it's a registrar that uses it, we would pick out a couple of domains and ask them to document that they actually did a full eID verification.

NICK WENBAN-SMITH Question over there. Yeah.

PIERRE BONIS Yeah. Thank you very much. Pierre Bonis for the record. Thank you for the presentations. I would like to know when you verify a new domain name and decide not to activate it. Do you charge it to the registrar.

KRISTIAN ØRMEN

Yeah, the domain will be completely registered, and it will just be an error to the registrar with a request to re-verify. And the domain will be in the registry until their expiry date so if they don't verify, they registered for a year, it will just be in this like server hold state for a whole year, or even 10 if they registered for 10 years. So, we don't see a reason to delete it, we invoice the registrar and they have all the time they need to see if they can fix it. And if not, it's just going to be blocked still.

PIERRE BONIS

Okay. And if the registrar decides to delete it, because he realized that the data is corrupted or is not good, will you charge the registrar or will you make it like a grace period?

KRISTIAN ØRMEN

We do charge for every registration; we usually don't credit. Sometimes if a registrar had been hacked, or registrant account and like a thousand domains was registered, then we would tell that registrar, okay, come in with an incident report, come and tell us how you are trying to prevent this in the future. And then like we can do like one-off credit note on a case like that, but normally we don't credit a domain that was already registered.

ROELOF MEIJER

Thank you. Rolf Meijer. Do you have any information on the effects or the impact on the number of maliciously registered domains under .se since you introduced eID verification?

KRISTIAN ØRMEN

Like I said, no, we don't. I don't think it have had any effect. I will go Deep Dive into those numbers, but it is a voluntary scheme right now. So, if you want to abuse a .se domain, you just choose to register without eID. So, I would say it's a good curve also that we already up to 40%. We have more registrars focusing on verification. We can see that we have like good data on these registrations and so on. But again, I don't believe it has any effect on the abuse level.

NICK WENBAN-SMITH

Okay, thank you. Is this initiative anyway connected with the NIS2 obligations?

KRISTIAN ØRMEN

Well, yes and no. Like since we started a long time ago, we of course know that there was going to be verification requirements in NIS2 and we wanted to start working on it early. But we didn't want to like put crazy requirements on the registrars early. Also, we didn't know the exact text in NIS2 was, so we thought it would be good to start with this incentive. You know, people could start working with it. We could see that it worked.

We also wanted registrars to do verification and we wanted to be able to showcase that that was possible. So, if there would be a requirement, for example, from EU and eID later, we could already showcase that this worked well in the registrar's order flow. And that we didn't have to put in a registry order flow since we generally

don't want to speak directly with the registrar because this is the registrar's part of the business in our mind. Exactly.

NICK WENBAN-SMITH And in Sweden, there is a national identity card, is there?

KRISTIAN ØRMEN More or less, everyone has this eID in Sweden. In the UK, whenever? I'm one of the few that don't. So, if we put in a requirement, I couldn't register that SE to win. But that's because I live in Denmark, so it's another story.

NICK WENBAN-SMITH Ah, what fun. In the UK, obviously, we talk about national identity cards, but as soon as any government suggests that they normally get elected out of power, so it's never come to force yet.

KRISTIAN ØRMEN So, I know my slides was maybe a tiny bit more than I should be speaking on, but let me get back. And just like this last thing, from the 1st of May, we're going to activate a new system where we can better work in big volumes on old domains. So, basically, what we can do if we find domains where we can see have some kind of weird data on it, we can just put those domains in the system.

The registrar will then get a poll message with a date where they have to re-verify the domain. Usually, we're going to go with 60 days unless there's something crazy on the domain. As an example,

we have 12,000 domains where we can see in the business registrar that the company doesn't exist anymore. So, domains like that, we're going to put in there. If we see domains in abuse feeds where we see that also the data looks wrong, we're going to give the registrar less days, for example, five, but depending on the case. So, it's flexible, but it's also good with volume, and it kind of follows the same path with new domains as before. Yeah, I think that was my last slide, if I remember correct. But at least, yeah.

NICK WENBAN-SMITH Okay, very interesting. I had a question for Reg, actually. Are you a .se domain registrar? Do you know?

REG LEVY Yes.

NICK WENBAN-SMITH How do you find it with all of the different CC weird rules and then the gTLD weird rules? Is it kind of fine, is it? You like the financial incentive and all is good?

REG LEVY I have a 10-person team that deals with compliance, and they almost exclusively deal with compliance for gTLDs because there are so many ccTLDs that we handle that we rely on a different team, the ccTLD team, to do a lot of the stuff there. So, if it's DNS Abuse,

it comes to us, but then if it needs to be suspended or anything else, often that goes to a different team. ccTLDs are very confusing.

NICK WENBAN-SMITH

Yeah, I mean, you just hear two quite different examples already. I just wonder, the challenge of having these different standards of the different ccTLDs, is that in itself a risk in terms of it makes it easier for bad threat actors to exploit the gaps between the different compliance regimes and the different rules in different places? As you say, it depends whether you live in Denmark or Sweden, what type of identification you can have.

And I came back to my original point, which is the vast majority of the registrations, especially in ccTLDs, are completely legitimate, even if perhaps some of the data is not as good as it could be. Fundamentally, these are legitimate registrations, and it's a cost and inconvenience which is being imposed across everybody. And does it make industrial logic, I guess?

REG LEVY

Yeah, so we find that most registrations are legitimate, regardless of what the registration data is. And it has not been our experience that we're targeted because we carry so many TLDs. Most people don't know that we exist because we are wholesale registrars. So, our primary .se customers are Swedish resellers. Our primary German .de customers are going to be a handful of German resellers. There are exceptions to a lot of these, but it's not the

sense that we get that people are targeting two cows for abuse because there are so many TLDs that are carried.

NICK WENBAN-SMITH: And what's your opinion, do you think there's a utility in registration data, either at the point of registration to prevent malicious registrations, or in response to complaints or phishing reports or feeds, you use the data verification process to take the domain name out of the DNS? Are you above average or below average on the 8.1, or is it all a pain in the ass?

REG LEVY: I was below average on the 8.1 because I don't see a correlation between so-called verification. I'll come back to that in a moment, and DNS Abuse or other types of abuse. And this can be seen as well with regard to, and I'm not going to pick on any ccTLD. I'm going to pick on .edu. .edu has extremely strict requirements for how you get a .edu. You have to be an entity. It's not just any rando. And it has wild levels of abuse. So, a lot of it's through compromised domains because the .edu is going to allow their students, allow a lot of open access to their domains and to subdomains and to URLs and that kind of thing.

So, there doesn't always seem to be a relationship between so-called accurate data and abuse. And I say so-called accurate because everybody determines accuracy differently. So, Kristiane has an eID and Barb has biometric verification. Those are completely different. And each of them is going to say it's verified

or it's accurate. But every TLD determines what that is in a different manner. So, when you say is accurate data useful for combating DNS Abuse, I first of all don't know what you mean by accurate data because there are differences within that. And secondarily, I don't see a correlation either in ccTLDs or in gTLDs between accurate data if we decide on what that definition is and the presence or lack of abuse.

NICK WENBAN-SMITH Okay, this is an interesting thought because a lot of us in the room spend a lot of time and effort making sure our underlying data are accurate because we think that as a registry having good, clean, accurate, up-to-date data is a fundamentally important point of principle.

KRISTIAN ØRMEN Just a quick add to that. I would just say we have a lot more inaccurate data than we have abuse. So, you can't say inaccurate registration is abusive registration. It's just two completely different things.

NICK WENBAN-SMITH Yeah, exactly. And I think a lot of ccTLDs, and I include the UK, if somebody complains about a domain name or complains about phishing or becomes alerted to something, the first thing you do is look at the registration data as a sort of a quick fix because it takes time and effort to investigate all of these sorts of things. So, if you

can quickly see that the registration data are wildly wrong, then that gives you a bit of a clue. Chris?

CHRIS LEWIS-EVANS

So, I'm going to go back to the start, and Chris Lewis for the record. The Menti poll was, is accurate data useful to combat DNS Abuse or abuse? What does combat mean? So, and Kristian said, accurate data is useful for police. And it is 100% useful for police. My view of combating abuse is to remove that abuse from online, number one, because that is them protecting people. How do I remove that abuse? We have suspension. Inaccurate data, a great way to tell this is probably a customer I don't want. They've entered completely false information. There's abuse. It's five days old. You will help the police most times to remove that, and great, people are protected.

Police have combated that DNS Abuse. But a lot of times, and especially in TLDs, you have long periods of registration for domain names. Certainly, what we see in the CCs is more domain names that are seven years old or older. And I think Reg mentioned the EDU case. And they're compromised domains. We don't want to suspend those as police. But to combat DNS Abuse on there, we can arrest the person that's compromised that. But guess what? That takes a long time.

If it's compromised, accurate data is not going to help us arrest that person. What is going to help us is to support the person that has been compromised to remove that data. Stick with the EDU, so I'm not picking on the CC. How does law enforcement support

someone that they can't contact? Because you don't know who they are. A lot of times you say, oh, you can go to the hosting provider, but that could be behind a CDN. I know you can go to the CDN and get that information. Or they might be hosting it themselves. That happens quite frequently.

And surprise, surprise, if you're hosting it yourself, you need to update everything. You need to keep stuff secure. People don't do that very well. That gets compromised quite quickly. So, accurate data is very useful from a police perspective to combat abuse so we can contact the person to support them to fix their systems. Remove that content and secure the systems is a really important part of combating cybercrime, crime, crime online, however you want to label that. And I think that's probably the biggest part of why accurate data is useful.

So, I would certainly recommend for CCs to keep doing it. On the flip side, it does provide a barrier or a friction point for registrations. Criminals generally are lazy. I can say this now because I'm no longer law enforcement. Criminals are lazy. They will go where it's easy, where it's cheap, where it has impact on the type of people they're doing. If you're asking for an eID or biometrics or some other form, they're going to go somewhere else if that's available.

If everyone had registration requirements, they're still going to come because they want to make money. It's a big business for them. So, is it the panacea to combat all abuse? No, definitely not. That abuse is still going to happen. Yes, it will help. It will stop friction. But for me, accurate abuse supports combating

cybercrime by enabling police and other people to successfully contact someone and support them in the removal of that.

NICK WENBAN-SMITH Okay, got it. I've got Reg and then Bruce.

REG LEVY Yeah, and to follow on from that, from my perspective, we focus on contactability. So, as long as we can contact our customer because so much of the abuse is compromised and we can help them get rid of the abuse, then that's what we care about. So, I often say this. I've got, like, 11 email addresses. Which of them is accurate, right? All of them can contact me, so any of them should be fine. But I'm often troubled by what seems to me to be some sort of, like, license to use the Internet.

We don't ask for identification when people are buying paper and stamps. But in some areas, we've started to drift toward, well, if you want to be able to express yourself online, you need to have some kind of identification. And that it's not just the ccTLD space. Like, this is certain social media sites are requiring similar things. And that concerns me greatly.

NICK WENBAN-SMITH Interesting. Bruce and then Pierre. Are there any questions in the Zoom room? Just rely on Yoki to keep an eye on it for me.

BRUCE TONKIN

Yeah, just a further comment on what Reg is saying. I think there's a very big difference between registration data that's in the same sort of timeframe as the new registration. So, whether it's, you know, on the day or within a few days or within a month versus registration data that relates to compromised domains. Because as Chris pointed out, we see on average they're probably names that have been in the system for more than seven years.

They're generally hosted on a content management solution that hasn't been patched. So, that's another common characteristic. And then often the registration data is out of date is probably the right word as opposed to inaccurate. So, it was originally accurate, then it's become out of date. And what registrants tend to do with registrars is they keep their billing information up to date, which essentially is their credit card. Most registrations are on some form of auto renewal. And then if the renewal fails, they update their credit card. They don't really look to update the rest of the information that the registrar holds.

So, it's a very different challenge dealing with the compromised domain scenario. And as Rich says, usually we rely on the registrars to contact the registrar using other data that they may hold.

NICK WENBAN-SMITH

I think as Chris said, it's a disruptive, you can disrupt criminal activity. So, it's one of the tools for disruption. And I think just because the existence of money laundering or anti-money laundering rules for banks doesn't completely prevent money laundering. It doesn't mean to say that we don't expect our

banking institutions to have a good stab at not being used to launder money. So, Pierre, next and then Reg, I think. Oh, Kristian, sorry. Kristian, Pierre, Reg.

KRISTIAN ØRMEN

So, just to follow up a bit on like focusing on the contactability. So, NIS2 with the original text, I thought they would be a lot more-strict. But the NIS2 corporation group came out with some recommendations to member states. They are non-binding. But what I found interesting was that the main focus they have is on email and phone number. And then they have some definition that I'm not sure how to interpret yet. But they say like for medium high-risk domain, then we recommend you to verify the actual name of the registrant as well.

So, how I read that is that basically they say that verification of email and phone number is the most important. We expect you to do that on all registrations. And we expect some registrations, do a more proper verification. Now, again, I'm not a lawyer. But I found it interesting that they actually had much less requirement in their recommendation than I was expecting in the start. And the contactability is definitely still the most important.

NICK WENBAN-SMITH

Well, my experience as a lawyer dealing with regulators is that you are judged in the rear-view mirror. If you have lots of abuse, then that is taken as evidence that you're not doing enough to do the verification. And so that's how it works. So, keeping a clean ccTLD,

apart from being obviously a public benefit to protect your communities and citizens, is also a good defensive action against a regulatory intervention. And I think I had Pierre been waiting very patiently.

PIERRE BONIS

Yeah, thank you very much. I just wanted to echo because this thing has been said already two things. The importance of reachability, contactability. And when we are talking about compromised domain name, the important thing is that you reach the registrant. That's not that you know that he's Pierre Dupont. And this is something that is far easier to do for registry to make sure that the registrant is answering than to make sure that the registrant is the person who pretends to be. First thing.

Second thing, I would echo what Kristian said. I mean, when we use the verification of the data to fight abuse, that's exactly what we do in .fr. This is our primary tool. I would say that more than 99% of the verification that we launch when we know there is an abuse show us that the data is rotten, that it's not a good data. On the contrary, most of the non-updated data or not exact data doesn't lead to any kind of abuse. And this equivalent between clean data and no abuse is not very convincing at the end of the day.

NICK WENBAN-SMITH

I had a question for you then about when AFNIC contacts the registrant around their reports or to do the verification, does the

registrant know who AFNIC is? How do you persuade them that this is not a phishing email in itself?

PIERRE BONIS That's a very good question because sometimes the registrant says, I don't know who you are, maybe you're a scammer or something like that. The thing is that we send that information or that request at the same time to the registrant and to the registrar. And so, if the registrant doesn't trust us, he should at least trust his registrar.

NICK WENBAN-SMITH Maybe. And sometimes the registrar on the record for the registry is not the same person that the registrant contacted because it could be a reseller or a web hosting company which then uses a registrar. So, sometimes it can be very confusing.

PIERRE BONIS And that's why you have a two-strike in our system. After five days, which is pretty short, we suspend. And then after 30 days, we delete. When you're suspended, you just go back to your emails and try to know why. And you contact maybe your reseller or your registrar and try to understand why your domain name is not working. And if you give the answer that we ask, in minutes you're online, you're back online.

NICK WENBAN-SMITH Okay. Because that's my other, my hesitancy in talking about registration data as a tool to combat abuse, combat, is that if you're a proper foreign state actor, proper threat actor, you are smart enough to do the bad registration, create mischief in the minutes and hours before any of these sorts of checks and processes can come into effect. And so, is it good enough? It's interesting and it's useful, but it's not the complete solution. So, Kristian and then Luc and Chris.

KRISTIAN ØRMEN Just a quick reply to that. So, we also use these checks. Now we do them together with registrars as well. We have to keep in mind that we have to protect the registrant also. If we give them a time frame of 24 hours, for example, that's just too little. Like they need to be a reasonable time to react. Of course, we have to look how bad is what we're looking at, and then maybe change the time frame based on that. But it really needs to be reasonable and they need to be able to provide evidence.

So, after suspension, they can get their domain working again and so on. It's super important also not to give yourself too much power. Again, we are not the police. We are creating policies that help the society with working on Internet domain names and so on. And the police let's be police.

NICK WENBAN-SMITH Exactly. So, very quickly, Luc, and then Irina, because you haven't said anything so far.

LUC SEUFER

Yeah. Luc, from your audience, it was just too hard, but yeah. That's the low-hanging fruit was the one that had incorrect data. And regrettably, I agree or don't agree with Chris. Criminals are all not lazy. So, if they want specific domain name, they will jump through many hoops you want to put before them. And to give some color, I hope I can say that here. I don't want to be thrown on a plane home early. We are reselling .cu, so Cuba. And those domain names require local presence, and we are retelling them for $1,200 per year. And still, we have got sometimes abuse there. So, yeah, there is no magical solution.

NICK WENBAN-SMITH

Thank you. Irina.

IRINA DANELIA

Hi. Irina Danelia, .ru, speaking. We are speaking about second-level registrations. Let's take this as an example. So, we attempt to verify data. We have processes and procedures to suspend domain names. But what we currently see that a lot of DNS Abuse is addressed by the domain names from the third or fourth or even fifth level. So, I would be interested to learn your thoughts on how should we deal with that. Should we still penalty second-level domain name holder and care about his data or other ideas?

NICK WENBAN-SMITH

I see Reg as a volunteer to speak to this.

REG LEVY

I'm going to not face you, but I apologize for that. So, yes, we would look to the second-level domain name owner. Because typically when the abuse happens at the third, fourth, fifth level, it's either because the domain itself was maliciously registered, in which case, I mean, the second-level domain was maliciously registered, which means we can suspend it, and great. Or it means that the second-level domain has been compromised because the DNS records start at the second level.

The person who has access to the second-level domain is going to have access to the third level and the fourth level and the fifth level. And I use the term second-level domain to mean the third-level domain in a .co.uk because we're selling .co.uk as the top level. So, even though that's technically third, second, yeah.

NICK WENBAN-SMITH

Thanks. Kristian, and did you? No. Okay. We are going to repeat the question. So, we're going to have enough time to do that. So, very quickly, and then we're going to repeat the poll.

KRISTIAN ØRMEN

Yeah, a quick follow-up. So, we have another industry player that sells top-level domains on .com.se. We get a lot of abuse reports on that, and, of course, we can't really do anything else than to point at the registry for .com.se to handle those abuse complaints. If we were to, like, shut down .com.se, we also will shut down, like, actual businesses' websites. A recent example was Five Guys

started a burger chain in Sweden also now, and they couldn't get FiveGuys.se. They registered a FiveGuys.com. e. So, there might be many other top-level domains on .com.se that are problematic, but there's also very good domains on it, and we can't just, like, suspend the whole zone.

NICK WENBAN-SMITH: There's a sort of proportionality element to it. Did you want to say something briefly, Chris? And then we'll get ready to do the poll thing after this.

CHRIS LEWIS-EVANS: Yes, just very quickly on the point from AFNIC is if you email someone, they either don't know who you are or don't believe who you are. So, having multiple points of accurate data for contactability is really important, especially in compromise. If their email address is the one that has been compromised, you can't guarantee contactability via that mechanism. So, having accurate data across all the contact points is really important, not just that single email. And that becomes even more important when that is linked to the domain, because if you suspend it, you can't contact them via that email address.

NICK WENBAN-SMITH: Well, I've seen that before with domains which I've suspended, and I just sort of roll my eyes because I see that the email contact for the domain registrant is the same domain that we're just about to suspend. So, his email is not going to work. So, that's not very

smart. Okay. Repeat the thing. Okay. So, I can see the numbers. I can't remember how many we had first time around. It was 41 participants. So, isn't life interesting? This is not what I was expecting. So, we have a long, deep discussion from experts about the importance of registration data, and the outcome is we think it's less important than we did at the beginning of the session. Did I just interpret that right or not?

KRISTIAN ØRMEN

We think it's maybe less important for abuse. Like, registration data is important for many people, but, like, as I put in my slide, it's not going to fix abuse. And I think that the fact that the score is lower now is just, like, saying that out loud also.

NICK WENBAN-SMITH

It's not much lower, but it is lower. And I think in my concluding comments on this, I would say one of my favorite books is about sort of clinical trial data and medical evidence. The title of the book is called I Think You'll Find It's a Bit More Complicated Than That. I think with the whole thing about registration data, DNS Abuse, the definitions, the problems, the contactability, the complexity of the ecosystem, the different rules in different geographic places, the smartness of the threat actors, the ingenuity of people who are incentivized to make money through criminal means, it is a bit more complicated than it might seem at first instance.

So, that is actually the end of the official session. So, I just want to thank everybody, actually, for a really good engagement and

participation. If there's anybody who didn't want to say anything that wants to, I'm very accessible and easy. I'd be super interested to find out how our newcomers enjoyed the session or hated it. It's still here at the end of it, which is good, I guess, positive. But, yeah, thank you very much, everybody, and thank my excellent panelists.

[END OF TRANSCRIPTION]