ICANN67 | Virtual Community Forum – At-Large Policy Session: DNS Abuse: An At-Large Call to Action
Monday, March 09, 2020 – 13:45 to 15:15 CUN

MICHELLE DESMYTER: Good morning, good afternoon, and good evening, everyone. This is Michelle DeSmyter from At-Large staff. Welcome to the ICANN 67 virtual meeting and the At-Large policy session, DNS Abuse: An At-Large Call-to-Action Virtual Session on Monday, the 9th of March 2020 at 18:45 UTC.

The Zoom room audio is in English. In order to access the French or Spanish audio, please join the French or Spanish streaming via the link on the main ICANN 67 website. All details were sent out on the ALAC Announce list with all relevant links. Details for these connections can also be found on the ICANN 67 At-Large Wiki agenda pages.

We will not be doing a roll call today for the sake of time, but ALAC members, RALO leadership, and liaison attendance will be noted. If you would like to ask a question or make a comment in English, French, or Spanish, please type it in the chat by starting and ending your sentence with question or comment, and please keep them short if possible. French or Spanish questions will be translated into English and read aloud by a remote participation manager. First name plus last name.

Staff will put periodic reminders of this process in the Zoom room chat. If you are in the Zoom room and wish to speak, you may also raise your hand and staff will manage the queue.

As a friendly reminder, please state your names when you speak not only for transcription purposes but also for the interpreters to identify you on the audio streaming. Please also speak clearly and at a reasonable speed to allow for accurate interpretation.

Finally, this session, like all other ICANN activities is governed by the ICANN expected standards of behavior. I will go ahead and put a link in the chat momentarily to those standards for your reference.

So, without further ado, I will hand the floor over to Jonathan Zuck. Jonathan, please begin.

JONATHAN ZUCK: Thanks. And thanks, everyone, for participating. 164-165 participants. That's really exciting. The ALAC have made the decision to make DNS abuse one of the principle topics for the At-Large for 2020, so the idea of this session is to kind of get an overview of some of the topics around DNS abuse, so this will be rudimentary for some of you, new for some of you, etc. But it's kind of a DNS abuse 101 discussion about what the different kinds of abuse are, what DNS abuse is, and some of the challenges that are faced around decreasing the amount of DNS abuse.

Finally, a call to action and a plan for the At-Large to take this on as a campaign for the year moving forward. In the agenda, you'll see that there are links to videos of this presentation in English, Spanish, and French. So, if any of you are having Zoom connection difficulties, these videos are available on YouTube and you could watch from the

YouTube links instead of the Zoom if you're having trouble holding on to a Zoom connection or having bandwidth issues, or if you want to go back and watch them later on, they're available in all three languages and they're linked in the agenda.

So, what we're about to do is play a video—the English version of the video—and we'll have French and Spanish translation on the Zoom call but feel free to use the links in the agenda to watch it on YouTube if that's easier for your connection.

So, without further ado, staff, if you would play the video, that would be a great way to begin. Thanks.

JONATHAN ZUCK: [Jonathan Zuck in video] Good morning, good afternoon, and good evening. Or for the less fortunate, good middle of the night. ICANN policy development is deceptively complex. Given the relatively simple mission of the organization, it's easy to miss the big issues when we're buried in the little ones. As the only representatives of the interests of individual end users, it's critical that we do not lose focus. Instead, we must identify the biggest issues facing those individual uses and be persistent advocates for improvement in those areas.

Perhaps the pernicious threat to end user interests is DNS abuse. Today, we're going to talk about DNS abuse so that it becomes a part of every conversation we have in the ICANN community. Instead of the old expression, "What have you done for me lately?" the At-Large greeting will be, "What are you doing about DNS abuse?"

So, what is DNS abuse? DNS abuse is a term that gets thrown around quite a bit and has been the subject of much debate inside ICANN. In fact, after the review of the Competition, Choice, and Trust, the Board has initiated yet another community effort to define DNS abuse, so that they might better design a plan of attack.

Ironically, even using the most conservative definition on which everyone agrees, we can begin to design a framework to combat DNS abuse and simply use it more often, as the definition is expanding.

We're all pretty familiar with the DNS, or domain name system, by now. It's a fairly sophisticated system of questions and answers that gets you to where you want to go on the world wide web. It's a bit like a scavenger hunt where you need to ask one person for the name of the person who knows the number of the person you want to reach.

Of course, as they say in the movies, all that asking around can get you noticed by the wrong people. Just ask Dorothy as she asked around for wizard.oz.

Simply put, DNS abuse is a tax on or the criminal use of the DNS. Some people will try to parse this definition further by calling a tax on the DNS DNS abuse and attacks using the DNS, DNS misuse. But for our purposes, we're going to call it all DNS abuse.

One of the best-known attacks on the DNS is a distributed denial of service, or DDoS, attack. Here, there's a predator that uses a network of zombie computers to make so many requests that a server is overwhelmed.

Sometimes, a criminal element gets in between you and the servers from which you request information. This can be done with a so-called man-in-the-middle attack or DNS cache poisoning.

Simply put, the idea here is that your queries are intercepted and you're given the wrong number for the site you wish to visit.

These server-side redirects can be used for something called a farming attack, sometimes called phishing without a lure. Here, you're simply redirected to a site that looks like the one that you intended but is just set up to capture your log-in credentials. You think you're logging into your bank, but really you're just filling in a form for hackers to go and use on the real bank website.

One of the most common abuses using the DNS is phishing. A far less technical way to get you to the wrong server is simply to ask you to go. In this case, you receive an email suggesting something is up with your bank account and that you need to log in to fix it. However, when you click that link, you're taken to a farming site. This process is called phishing because you are lured into the fraudulent site.

Here's an example of what such an email might say. You can see that there are some key elements to such emails. Some kind of crisis for the short time to remedy, so that you don't think about it too much. Then a call for you to log into your account. Of course, taking you to a fraudulent site isn't the only use of emails. Sometimes, they have attachments that contain malware directly.

One area of particular concern to the At-Large is internationalized domain names (or IDNs)—those domain names using non-Latin characters. These relatively new domains are essential to get the next four billion users on the Internet. 70% of the world uses non-Latin alphabet. Finally, in 2012, we got the ability to register domain names in languages such as Russian, Arabic, and Chinese.

Of course, with every new innovation comes matching innovation by the criminals and individuals were no different. It turns out that a lot of letters in non-Latin alphabets look a lot like letters in Latin alphabets. Who knew there were so many ways to spell Bank of America? When someone sees one of these spellings while quickly reading an email, why wouldn't they go ahead and click?

In addition to collecting your credentials, these fraudulent emails and websites have as a primary objective to plant software on your machine. This software is broadly called malware but there are many, many different varieties in malware.

You've heard these types of programs before and many of you—or your friends and family—have fallen victim to them. While we don't have time to go into each of them in detail today, suffice it to say whether it's spyware or ransomware, you don't want them on your computer. Unfortunately, malware infection is on the rise. In the last ten years, malware infection has gone up nearly 700%. As an example, ransomware attacks have risen 350% in 2018 alone.

In fairness, especially after the review of the 2012 round of TLDs for Competition, Choice, and Consumer Trust, the folks in ICANN Contract

Compliance are doing their best. The Compliance team began publishing more and more granular data about complaints and began to make its audit process a little less random. But it's still not enough.

You might have heard something called the Domain Abuse Activity Report, which ICANN began a few years ago. While the monthly reports provide just enough data to know there's a problem, they don't provide enough to do anything about it, such as avoiding a domain or registrar that seems to be up to no good.

However, using DAAR, we can determine that the percentage of infected abuse has gone down less than 1% since its inception two years ago.

So we can all agree that DNS abuse is a major problem for individual users, but what can the At-Large do?

The At-Large will take a two-pronged approach to combating DNS abuse—outreach and ICANN policy development. The At-Large will develop education materials for end users to better protect themselves against DNS abuse. The At-Large is unique in its structure, making it possible to distribute information to the regional At-Large organizations (or RALOs) who in turn can distribute those materials to the At-Large Structures, each of which have individual members to which they can finally distribute the materials. The At-Large has been developing this network for years and what better use than to protect users from criminals on the Internet? There are a number of messages we can deliver to help people avoid the traps being sent to them every day.

It's the enduring irony that criminals get most of the information they need from users, not by being clever computer engineers, but like in the movies, by being clever social engineers. In short, if they want your password, they basically just ask for it. This was true before the Internet and it remains true today.

The At-Large needs to educate users to be on the lookout for news that's too good or too bad to be true. There are always ways to figure out whether an email is a fraudulent one or not.

We like to make fun of those phishing emails because of their bad grammar. What we don't realize is that bad grammar is intentional. Writing this way simultaneously triggers a deletion by those who recognize the scam and sympathy from those who are less sophisticated. The At-Large can certainly help end users to discern the authenticity of an unexpected email.

It should go without saying, but the At-Large will say it anyways, that individual users should have virus protection software on their PCs and mobile devices.

In fact, in the United States where you would expect considerable sophistication by users, nearly 50% of computers lack virus protection. The At-Large must encourage end users to ask their employers if they have DNSSEC-enabled servers to prevent events such as man-in-the-middle attacks.

The other place the At-Large needs to be heard is in the hallways, meetings and conference calls that make up the ICANN policy development process.

The At-Large will engage in ICANN policy development at every point of entry. In one case, it might be a conversation in a hallway or participation in work group or review team. We will actively engage in advocacy for reforms both inside ICANN and among the businesses that serve end users, such as registrars and registries.

In other words, if someone asked us about the weather, we will stick out our hand, look up at the sky and say, "It feels like DNS abuse."

Thankfully, we're not alone. The majority of the ICANN community is concerned about DNS abuse and hesitant to allow a new round without significant reform. There's simply no way that a minority of voices should be able to drive ICANN to a new round without real buy in from the rest of the community. The At-Large has and will continue to partner with other groups within the ICANN community to sound the alarm regarding DNS abuse and actively promote reform.

Our first task is to simply hold the line. There should be no new round until DNS abuse is addressed in a meaningful way. Compliance [inaudible] a holistic view of DNS abuse. They cannot simply react to complaints but misuse their audit power to recognize high percentages of abuse and take action against TLDs, registries, and registrars who are part of the problem.

We need to limit volume registrations because there's a high correlation to DNS abuse. Of course, there are legitimate uses for bulk registrations and such uses will only increase with the Internet of Things, but the At-Large will continue to advocate for increased friction for such activity, perhaps requiring authentication as a legitimate bulk registrant.

The CCT Review Team, and consequently the Security and Stability Review Team have both suggested that ICANN design incentives to adopt best practices. The At-Large will continue to advocate for such incentive.

Certainly, more research can be done and has been recommended by the CCTRT, the SSRT, and ALAC and now Verisign. There's now essentially $20 million more in the budget to invest in security and stability of the DNS.

There are certainly those registries and registrars that investing significant time and money in combating abuse. In fact, 48 companies have signed on to a commitment to best practices. That's awesome. But we still need reforms to better address the bad actors, and frankly even the good actors could be doing better so the At-Large won't be easing up on those guys anytime soon either.

It's like that old Dilbert cartoon in which we were reminded that once everyone has adopted so-called best practices, those practices become the new normal and are no longer the best. The criminals are not satisfied with the status quo and neither can we afford to be. So, even the good guys can do better.

All that is to say that this is a crisis from which no one is immune. Incredible research is happening and machine learning to better detect abuse in real time and to predict that a registration is intended for illegal use.

Early tests of such technology by DotEU show a nearly 80% accuracy in such predictions. We need to ensure that such research continues and systems are put in place to protect us from the next generation of attack. When all is said and done, there's really only one constituency—end users. It's the interest of those end users the At-Large was created to advance. DNS abuse effects all of them. Say it with me. We have no use for DNS abuse.

Go to atlarge.wiki/dnsabuse for more information. Thank you.

JONATHAN ZUCK: All right, folks. Thanks for watching the presentation. We can go ahead and show you the DNS abuse page if you like, so you can see what's there. It's just the beginning but we're going to have a central home for the work that we're doing on DNS abuse. There under resources you'll see the three videos if you want to go back and review what you just saw in English, French, or Spanish, the links there for the YouTube versions of these videos.

So now I wanted to open it up for questions. Alan Greenberg, go ahead.

ALAN GREENBERG: [inaudible] but it's a great example of the kind of thing that we've been looking for ICANN to produce for forever now and I'm delighted to see that we've taken the lead on it. Thank you.

JONATHAN ZUCK: Thanks, Alan. Volker, go ahead, please.

VOLKER GREIMANN: Thanks, Jonathan. I think it's a good effort to go against DNS abuse. However, you might have also mentioned that registrars and registries have already, since last ICANN meeting, been very public about having published framework about DNS abuse which can be found at—let me look that up—dnsabuseframework.org, which basically details how many of the biggest registries and registrars are already handling DNS abuse and many of the abuse cases that you have detailed there are already being taken care of on a regular basis by these parties. So, thank you for that demonstration which details a problem that a lot of us are already dealing with on a day-to-day basis. Thank you very much.

JONATHAN ZUCK: Thanks, Volker. And thanks very much to the group of registries and registrars that have signed on to those best practices and those who are already doing them. I think the signatories are maybe a combination of those two things. I did mention it. I didn't know about the new DotOrg website, so thanks the dnsabuseframework.org. So, let's all check that out.

I did mention it briefly in the session in that there are registries and registrars who are doing much more than others to combat DNS abuse and I definitely wanted to draw attention to that fact. The problem is the bad actors and how best to address the DNS abuse on those in those TLDs or those registrars, which I think we all can agree exist.

So, the issue then becomes how to deal with the bad actors in a way that doesn't unduly burden the God actors. I think that's going to be an open topic for conversation. But with DNS abuse on the rise, it's clear that it's still a problem despite your best efforts and the best efforts of the 48, we can call them. We look forward to seeing even more best practices from you all. Thanks for what you're doing and we're going to keep fighting for ICANN to do a better job of dealing with the bad actors. Natalie, please go ahead.

NATALIE: Thank you very much. A well-put video, I must say. It was very informative. Would you be able to make a recommendation to have the DNS abuse on the ICANN Learn as a module?

JONATHAN ZUCK: Thanks, Natalie. I think it's a great idea and it's one of the things that I think we'll consider doing. We're trying to figure out what the best outreach plan should be. It could be part of ICANN Learn. It may be a dedicated website for end users.

I mean, the irony of a lot of this is that education could play a very large role in mitigating the effectiveness of DNS abuse, because it very

often involves tricking people. It involves getting them to give up their passwords or clicking on an attachment from somebody they don't know, etc. I think that that's something that we need to work on and ICANN Learn might be part of that.

I want to give the floor to Joanna for a second who is currently working on an ICANN Learn course on At-Large policy development and perhaps she can expand a little bit more of using ICANN Learn in this context of DNS abuse. Joanna, go ahead.

JOANNA KULESZA: Thank you, Jonathan. I'm really glad we have good participation and I'm really looking forward to the comments, so just let me be very brief. I noted this in the chatroom and I look at these sessions as outreach sessions as well, so if anyone has questions, please just reach out directly.

But as briefly mentioned, we are working on an ICANN Learn course that deals with the basics of At-Large policy advice, development, etc. DNS abuse is high on our agenda, so one of the avenues we are looking into is providing an ICANN Learn course that would deal with DNS abuse. I mentioned this also in the chat. We want to make sure that the language we use is comprehensible also outside ICANN. So the DNS abuse acronym already is an acronym. It has an acronym in it. So we would put a lot of attention into making this clear and understandable and easy to digest with linking that to cybercrime and cybersecurity.

So, I see a great potential in transposing the brief presentation, wonderful and very appealing by Jonathan as a course that could be incorporated into ICANN Learn, but also onto other resources we would make available to the entire community working closely with the RALOs to make sure that we are able to best address local needs and local expectations.

So, that would be the overall plan in terms of capacity building, providing the resources and that plan includes an ICaNN Learn course. But as already said, I welcome the feedback within the Capacity Building Working Group. Contact Alfredo or myself directly or just join one of our calls. Thank you so much.

JONATHAN ZUCK: Thanks, Joanna. Yeah. We welcome all kinds suggestions on what the best way is to reach the most people with these messages. So this could be a module of the course we're already developing or something special that's out for a broader audience or there might be a dedicated site as well. Those are conversations we're still having internally. Natalie, I'm assuming that's an old hand.

NATALIE: I'm sorry, I need to put it down. Sorry.

JONATHAN ZUCK: Yeah, no problem. Russ, please go ahead.

RUSS MUNDY: Thank you, Jonathan. Russ Mundy here. As some folks know, I've been promoting DNSSEC for quite a while and I was really glad to see that it was included in the presentation because indeed it is one aspect and a capability that will lessen the effectiveness of some of these people that are going to do the DNS abuse.

The one thing inside noticed, if I heard it correctly, was that the text around or the words around DNSSEC were encouraging people to ask their employers to make use of it. And that's good. Enterprises and employers, of course, should do that. But it's I think just as important—and particularly from an ALAC perspective—it would seem very appropriate to also ask as individuals that our Internet service providers also provide a service that is DNSSEC enabled. And any websites or service providers themselves, that they sign their zones so that it will be much harder to do a phishing attack or some malicious DNS abuse based attack.

So, I think at the risk of sounding like I am beating the DNS drum—in general I am—I think it can do more to help in the DNS abuse area than is currently described in what is one of the best DNS abuse presentations I have ever seen. Thank you.

JONATHAN ZUCK: Thanks, Russ. And very good point. I was trying to think about what to ask end users to do but talking to their ISPs and maybe even some of the websites they use is certainly a good suggestion. So, as we build out these end user education resources, we'll definitely take that point on and make sure that's part of the call-to-action for the end users to

reach out to ISPs and their favorite websites as well. So, thanks, Russ, for bringing that up. [Ephraim], please go ahead.

[EPHRAIM KENYANITO]: Hi. Just to go back to one thing that was mentioned about the automatic machine learning detection of DNS abuse. I just wanted to find out. you mentioned which registries. I just wanted to know so that I can follow-up. It's good for research.

JONATHAN ZUCK: Sorry. Which registries are doing what? Say that again?

[EPHRAIM KENYANITO]: The automatic detection of DNS activity.

JONATHAN ZUCK: Oh, definitely. It's DotEU that is leading the charge on that and have done significant research. I think that DotUK is starting to experiment with it as well. There is actually a pretty good white paper on the DotEU experiments that goes into real detail in terms of their methodology and the success that they're having with the predictive analytics. So, do a search on that or I can make sure and add it some place on the agenda or something like that that you can find as well. But yeah, there's a good white paper out from DotEU on those efforts of predictive analytics that we would really like to see more research go into that and see that become a best practice in addition to the

ones that we are seeing from some of the great actors that have signed on to the DNS abuse framework.

[EPHRAIM KENYANITO]: Yeah. Just to follow-up on that. Is it only those two registries or those are the only two you are aware of? I'm just curious if there are other registries in Asia or other parts of the world that are doing that?

JONATHAN ZUCK: It's my understanding that they're the only two but I don't know that for sure. I think the research is happening at DotEU. There is some also very interesting machine learning research coming out of Asia as well. If you email me, I'll share that with you. We made reference to it actually in a recent comment to ICANN Org on Valentine's Day. So you should be able to find it from February 14th. We made reference to this research as well which is about real-time identification of DNS abuse as it's occurring. So, it's different than predictive mechanisms, but there's some great research coming out of Asia on detecting DNS abuse in real-time, and that's coming out of Asia. Those are the two that I'm most aware of.

[EPHRAIM KENYANITO]: Thanks so much.

JONATHAN ZUCK: Laureen, please go ahead.

LAUREEN KAPIN: Hi, folks. I'm speaking in my capacity as someone who works as a lawyer at the US Federal Trade Commission focusing on consumer protection. I'll put this in the chat but I wanted to share that the ftc.gov site—easy to remember because you can think about '"for the consumer", ftc.gov—has great educational materials on how to protect yourself online and that includes materials that specifically tell you how to spot and avoid phishing attacks. These materials are almost always available in Spanish and English, and also if your organization wanted to use these materials and slap your own logo on it, we make it easy to do that, too.

So, I just wanted to encourage people to check out those educational materials because they are written by folks who are experts in creating user-friendly messages that are easy for people to understand. Even if English or Spanish isn't their first language, they're very effective materials. And if anyone has any questions about that, they can feel free to contact me offline.

JONATHAN ZUCK: Thanks, Laureen. If you would, go ahead and put a URL to those materials in the chat. I'm sure people will find that interesting. We will certainly take you up on the offer of rebranding some of them as we try to put together the resource information. One of the things that At-Large has an advantage over a lot of the other constituencies is a pretty extensive framework of organizational participants. So, there's the regional At-Large organizations. There's five of them, in North

America, Latin America, Africa, Europe, and Asia-Pacific. Then underneath each of those regional At-Large organizations are hundreds of so-called At-Large Structures which are often small non-profits, as well as individuals, that are members of each of those RALOs.

So, we intend to use this phone tree, if you will, to reach out to end users and help them see these materials. So, when there's great materials for people to see, we'll be forwarding them and we'll be creating some of our own and then using our network to get them out to the public. Marita Moll?

MARITA MOLL: Thanks. I think it's a terrific video. It will reach some people who are already fairly at a high level of knowledge of what's going on and what they're doing. There are so many different levels of knowledge for people that need to hear more about what not to click on.

I think our goal here is really to do everything we can to make sure that those messages don't get there in the first place. Try to put as many processes in place to keep those messages out of your neighbor's mailbox and your own because we all get caught in some of this sometimes. Thank you.

JONATHAN ZUCK: Definitely, Marita. This video is not the one that we'll be using for end user education. We'll be working on other materials for that. This is definitely aimed at At-Large participants or potential participants to

get them engaged in this campaign and get everybody excited about taking on the banner of DNS abuse for the upcoming year as a big At-Large topic. [Ephraim], do you have another question or is that an old hand?

[EPHRAIM KENYANITO]: Sorry. It's an old hand. Let me just get it down. Sorry.

JONATHAN ZUCK: Okay, no problem. Mason, please go ahead.

MASON COLE: Hi, Jonathan. Thanks very much. First, I want to applaud you on the video. It's very well done and I look forward to seeing that in other places on the web. I just wanted to call to the attention of the ALAC that the BC (the Business Constituency) has been fairly active on DNS abuse for the last five or six months. We published a statement before the Montreal meeting that I encourage you to have a look at on the correspondence page of the website. If I have time I'll put it in the chat.

Then there was an exchange as well between the BC and the ICANN Board recently on the subject of what can be done in cooperation with the contracted parties to address DNS abuse, and I'd like to call that to the attention of the ALAC and invite the ALAC's further support, if you're willing, on being a bit more activist in terms of advocating to ICANN the organization to do something proactive about DNS abuse.

JONATHAN ZUCK: That's great. Thank you. And we look forward to working with you guys. We've seen some of your comments and know that you have individual members that are deeply engaged in protecting your customers. I think there's a lot of points of cooperation between the At-Large and the Business Constituency on this issue. So we're looking forward to doing that.

MICHELLE DESMYTER: Jonathan, we do have a comment from [Steiner Groddard].

JONATHAN ZUCK: Oh, perfect. Go ahead.

MICHELLE DESMYTER: Okay. His comment is, "ICANN has web forms for WHOIS inaccuracy complaint form. Not very easy to check and verify due to the temp.spec/GDPR. Could it be a good idea to ask ICANN to enable a way to report abuse from their website? Note there is a site on about spam, phishing, etc." He has a website in the chat as well.

JONATHAN ZUCK: Thank you. I don't see the link in the chat but it may have scrolled past me. Definitely let's look into those possibilities as well. Obviously, WHOIS is starting to be something that's taking a different shape as a result of GDPR and the efforts of the EPDP. But we remain focused

from a policy standpoint on making sure that as much as possible can be automated, that the process of reputation engines and consumer protection agencies have the most frictionless access to that data so that they continue to provide the services that they do in combating DNS abuse.

MICHELLE DESMYTER: Jonathan, we do have another question.

JONATHAN ZUCK: Oh. Please go ahead.

MICHELLE DESMYTER: From Ram Mohan. "Is this primarily a hygiene issue? Should be dealt with [inaudible] is in real life? Wash our hands, install anti-spam filters, don't touch your face, don't click on random links in email, etc."

JONATHAN ZUCK: In some respects, it is for sure primarily a hygiene issue. There are certain types of DNS infrastructure abuse that are not hygiene issues or not as much end user controllable hygiene issues. That's where things like DNSSEC will help come into play, things like man-in-the-middle attacks, etc., are things that end users don't have the capacity very easily at least to prevent. But there's a great deal that end users could prevent through education.

That said, I think there's a lot that we can do by increasing the friction on bulk registrations, for example, and other things in terms of predictive analytics that could help give the end users a leg up because we all get into the habit of clicking on things that look familiar to us. So, if you see something that says Bank of America but one of the letters is not what it appears to be and it's actually an IDN that can be pretty difficult to decipher, even for a fairly sophisticated end user who is forging ahead.

So I think it's going to take the combination of efforts of those of us in the DNS community and education of end users to really see a dent in the level of DNS abuse. Are there other questions?

Okay. So, I was trying to look for interesting ways to make the all-virtual meeting a little bit different and more interesting. So, the next piece of the agenda is a quiz to help reinforce the topics that we learned on this and what we're after.

If you'd like to play along on some device—it could be your computer, your phone, you don't need to install any software—but you'll go to atlarge.wiki/daquiz and you shouldn't need to log in to do that. You should be able to just use the browser interface to go in and it will allow you to use your phone as a controller or your tablet or your PC. So, go to atlarge.wiki/daquiz. I can put it … Somebody put it in the chat. So, that's good. I will get the quiz going.

So, take a second to get ready and I will give you a minute to get ready to be answering questions and we'll start the quiz. So, hold on just a

second and let me figure out what I'm doing. Oh, I realize I muted myself. Sorry about that.

So, are people able to see the main quiz thing? Have I successfully shared my screen?

MICHELLE DESMYTER: You have, Jonathan.

JONATHAN ZUCK: All right. That's great. So, I'll just give people a couple more seconds to sign up. Basically, what will happen is that you'll see a question—a multiple choice question—and be given a few seconds, 20 seconds, to answer the question. You get extra points if you're one of the first people to answer the question correctly. Then you'll be shown the answer to the question after that before the next question comes up. So, I think we've got some people ready to go. I'm sorry I was muted. Hang on just a second and we'll get started.

Would anybody benefit from me reading this or is it okay for people—can people read it okay? Probably should have tried to find some way to incorporate some music.

SEBASTIEN BACHOLLET: Jonathan, you see we are 228, 229, 230 online and you have 60 respondents. What the others are doing? I'm not sure that it's best time we use. Okay.

JONATHAN ZUCK: Thanks, Sebastien. Just an experiment.

SEBASTIEN BACHOLLET: Yes, but an experiment with 230 people needs to be [inaudible].

ALAN GREENBERG: Those who aren't answering aren't having the fun of answering the wrong answers.

UNIDENTIFIED MALE: What's maleware?

JONATHAN ZUCK: Oh, is there a typo? Sorry about that.

ALAN GREENBERG: I don't know. I think I'm going to launch a politically correct suit against you.

UNIDENTIFIED MALE: I thought that wasn't a typo. That was intentional.

ALAN GREENBERG: I'm sure it was intentional. I think the first one is the right answer here.

UNIDENTIFIED MALE: So, which of these buttons installs maleware?

UNIDENTIFIED MALE: Shush!

ALAN GREENBERG: See, again, it's man-in-the-middle. They have something against us.

UNIDENTIFIED MALE: Well, what's your password, Alan?

UNIDENTIFIED MALE: Actually, that [works] in surprisingly many cases.

JONATHAN ZUCK: All right. Looks like we have a little bit of a leaderboard here. Thanks, everyone, for participating in this experiment in perhaps making the virtual version of ICANN a little more interactive and playful.

One of the other things that I'd like to do then as we wrap up is tell you about some of the other DNS abuse sessions that we have coming up. I'll start by telling you that there is a session on holistic tools for contract compliance. So, that's a session with Jamie Hedlund from ICANN Contract Compliance and James Bladel who is the head of policy for GoDaddy and they're going to be looking at a series of scenarios and what the best way would be for contract compliance to deal with that scenario and get both of their opinions.

Hopefully, what will begin to surface from that conversation is whether or not compliance has all the tools it needs to combat systemic abuse proactively as opposed to just responding reactively complaint by complaint. So that's one of the things that we'll be talking about in that session.

Then we have another session as well that I would like Joanna to introduce to you that's coming up later. So, Joanna tell us about your session and when it's taking place and what the discussion is going to be about.

JOANNA KULESZA: Thank you. Just a brief intro on Wednesday's session. We will try to talk about the ongoing discussions focused around cybersecurity and cybercrime. So, as already mentioned, a link to the DNS abuse discussion, but I appreciate the opportunity to work with Jonathan. He has a very compliance-oriented or business-oriented approach to DNS.

What we're trying to explore during Wednesday's session on "One World One Internet?" is the current debates around geopolitics, cyber sovereignty, the Internet public score or the ICANN remit would be right at the focus of that discussion.

We will be joined by Veni Markovski who just published a report on [inaudible] around cybersecurity and cybercrime. Leon has kindly agreed to join us as well. Patrik Falstrom will provide us with a brief background to the technical side of things. We're also looking forward

to welcoming NCUC participation with a debate on sovereignty, cyber sovereignty, and the possibility to draw lines in cyber space.

With that, Jonathan's approach to contractual compliance and his very pragmatic take on DNS abuse and training end users will find a reflection during Wednesday's session where we try to take a look at the bigger picture, looking at geopolitics that have been put on the Board's agenda for the next five years.

In that sense, as already briefly indicated, we would like to draw links between ongoing discussions outside the ICANN bubble that focus on issues that are of importance to individual end users when it comes to their security.

As already mentioned briefly in the chat, we would also like to explore the DNS abuse issue and its links with other end user interest. So, on one hand, we would like to explore what it is that end users actually expect when it comes to being safe online. We would also like to explore the links that there are between cybercrime, cybersecurity DNS abuse, and individual rights with reference to freedom of expression, privacy, intellectual property protection, etc.

So, Wednesday's session would be a look at the big picture as we have it with a question mark on the role that ICANN and its One World One Internet policy has and contemporary geopolitics.

Thank you for allowing me to introduce that session here and thank you, Jonathan, for this wonderful introduction into DNS abuse. I hope we will be able to contribute to the debate within ICANN but also

outside, beyond ICANN, when it comes to cybersecurity. Thank you so much.

JONATHAN ZUCK: Thanks, Joanna. I'm really excited for your session. That was going to be a big cross-community session in Cancun, so I hope that we'll get these kind of numbers of participants at your session. I'm really looking forward to it. Everyone make a point to get there. Then, later on today, we will have this session on holistic tools for compliance.

Staff, I think that's it for me, unless there are remaining questions in the other language queues, etc.

MICHELLE DESMYTER: One moment, Jonathan. I don't believe so, but just double checking. No further questions.

JONATHAN ZUCK: Okay, great. Thanks, everyone, so much for participating. Thanks, Volker, for pointing out the new site. Everyone take a look at that dnsabuseframework.org. Also, at the end of the video, you saw there was a website for where to go when the At-Large are working on these things to see what's going on there and that is atlarge.wiki/dnsabuse. So, go ahead and pay attention to that and follow along with what we're up to on that page on the At-Large website.

Thanks so much for everyone participating. We really enjoyed it. Thank you so much.

MICHELLE DESMYTER: Thank you, Jonathan, and thank you everyone. The meeting has been adjourned.

UNIDENTIFIED FEMALE: Thank you, everyone.

[END OF TRANSCRIPTION]