ICANN82 | CF – Joint Session: ALAC and SSAC
Sunday, March 09, 2025 – 13:15 to 14:30 PST

MICHELLE DESMYTER: Thank you. Hello and welcome everyone to the Joint Session, ALAC and SSAC. My name is Michelle DeSmyter and I'm the remote participation manager for this session. Please note that this session today is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for this session today will include English, French, and Spanish. If you would like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. 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. I will now hand the floor over to Jonathan Zuck, ALAC Chair, and Ram Mohan, SSAC Chair.

JONATHAN ZUCK: Ram's missing, I guess? I am Ram, coming from the darkness. So, I want to repeat what Michelle just said. This is a very heterogeneous

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

group here in the At-Large community, so I really recommend that you unwrap your headphones and actually plug it in and choose your language and that sort of stuff now so that people can make a quick transition when they decide to speak in a language other than English. It's worth doing it up front.

And meanwhile, I'll talk a little bit about the ALAC and the SSAC. We are, I think, finding ourselves aligned on a number of different issues, and it's been a really good and fruitful partnership that we're only beginning to scratch the surface of. We did a joint correspondence to the Board and have already received a response on that, and working together on this DNS phishing education campaign that we've finished the course of and now need to start the process of getting it translated and then out to the field to deliver these courses.

And so, we're always generally excited about the things you're working on, and I think we both focus a lot on DNS Abuse and finding answers there. I don't know whether or not you shared our frustration with the webinar in INFERMAL, which essentially said we found all these correlations, but you shouldn't do anything about them, which was a strange call. So, I'm looking forward to talking about your thoughts on that study. But thanks again for being here, and welcome. And you're the substitute Ram, right? So, introduce yourself to the group and say hello.

JEFFREY BEDSER I'm the substitute Ram Mohan. I'm Jeff Bedser. I'm one of the leadership team for SSAC, and as the core topic of discussing the

INFERMAL Findings is under the DNS Abuse category, and it's one of our core topics for SSAC, and I'm the topic lead. I'll be taking that category in this conversation.

JONATHAN ZUCK

Cool. Let me see. What we put on the agenda was, I just want to make sure I'm setting this up correctly, a little bit of look at what this course is looking like, so you can see how this is coming along. And so now, with any luck at all, I can come into Zoom and share my screen. I'm going to replace the current share, just give a heads up to staff. So, it looks a little bit like this, although this is very high contrast. So, it's a little more colorful than this, but we'll go through it, and we'll see a little bit of what it's like.

So, it gets into some high-level numbers at the outset about how this problem continues to grow, and talks about different types of cybercrime, and then phishing is the one in which we're focused on primarily for this course. We're going to look at a little bit about what phishing is, how to identify phishing attempts, and then how to prevent, and if you're feeling particularly altruistic, perhaps report it, so that it doesn't reach somebody else.

And so, we talk a little bit about what phishing is, what the steps are. You target a user, you put together some a farming site with a login screen, and then you're directed to that farming server instead of the one that you thought of. This is obviously all stuff that you all know. And you get an email or something else directing you to that particular site.

So, this might come from Bank of America, you click on it and you find yourself at the Bank of America website, and you fill in your login information, and then if they're smart, they forward it on to the real Bank of America site, and they're done because they've captured it. It's like the veneers they used to put on ATM machines, it still worked, you still got your money. You didn't feel like anything had happened, but your information had been captured.

So, we'll talk a little bit about the different types of phishing, this is going to be fun. I did a class for the North American regional At-Large organization about phishing, and actually did a little bit of spear phishing on the chair, by researching where he went to school, and what the name of the quarterback was the year that he was there, and then sent him a fundraising letter from the quarterback pointing him to a site that looked like their alumni fundraising site, so that you can really-- He was shocked at how much information was available about him on the line for me to particularly target him.

Phishing was something that we added recently at request of Ram, and I'm getting more and more of them, so it's certainly relevant. So, you can see this is the run of things. We talk about the emails themselves and how they're constructed, suspicious sender, really urgent language requests for personal information. And then we go through and break down some actual emails, some actual phishing emails and show how these different aspects show up in those emails, and so I think this is something we'll do even more of and do in multiple languages as this evolves.

And then talk a little bit about malware, toll-free number, another place that people get sent instead of a website, touch on malware, but we're mostly talking again about phishing. I'm trying to be a little bit comprehensive. And this is about the customer support representatives. Things you shouldn't do. How to look at URLs, hovering over them, look, checking to see where that URL is actually pointing, things like that is the idea behind these examples and tips.

And then you may be familiar with the fact that Google at one point, they put together a phishing quiz with Jigsaw, exactly. And it's in multiple languages and ready to use and quite comprehensive, so we thought in the middle of the class we'd send people to that at their desk to try it out. And we talk about different types of phishing, things you might do to prevent it and report it. Just to give you some sense without bogging it down, but I'm happy to share this with you as well. One last time, we shared an earlier version, but I think this is close to done, so it would be a good time to look at it again.

A little bit of a summary of what we went through at the end, and some URLs and the QR codes to get to places to report things, and that's something we talked about yesterday. We'll need to localize, right, the people in France shouldn't reach out to the FTC necessarily, so we'll have to go through that. But that's basically the course in a nutshell that we have to push out through our infrastructure, which is regional At-Large organizations, and then in turn their members, which are called At-Large structures, about roughly half of which are ISOC chapters, and the rest are other

organizations that at least have some interest in ICANN activities and have shown some interest in participating in the things that we've done around universal acceptance, for example.

And we also have beginnings of a relationship with the International Library Association, who are also interested in teaching this course, because they're doing more and more of that sort of community outreach in libraries, since nobody reads books anymore. Libraries have become community centers basically. And they were excited to see that a multilingual course could be made available to them as well. So, happy to call on folks with their cards out.

BARRY LEIBA This is Barry Leiba. This is something you might think about tweaking. So, you mentioned the personalized looking email with colloquial language and hi, good to see you, or whatever. In the last month I've been at the MOG meeting, Messaging Anti-Abuse Working Group, and NDSS, the Network and Distributed Systems Security Symposium. And at both of those, there was discussions about something that we've seen a lot of lately, with hyper-personalized stuff that's targeted in ways at scale that couldn't have been done before through AI.

And it collects information about everybody and makes personalized messages that used to be only practical to send to the company president, but now they can send it to Jonathan and me and Matthias and everybody. And you're getting messages that they know where you live, they know where you work, they know

what you do, they know what your hobbies are, and they really are hard to tell from real messages. So, that may be something you want to tweak here of how bad the problem is, and how even savvy people are fooled by this stuff.

JONATHAN ZUCK Oh, sorry, I just turned it off, just in time to speak. Me and microphones, I'm so high-tech. If you have examples that you can share, that would be great as well. I've yet to receive, I feel kind of bad, I haven't received a highly customized--

BARRY LEIBA Yeah, you and I don't rate.

JONATHAN ZUCK Right. And I'm sorry about that, because I could contribute. I could buy you Bitcoin, I don't understand why I'm being left out. So, I would love to see one of those. I've only heard about them and people talking about them, and I created one, like I said, from scratch with only my own people intelligence.

BARRY LEIBA I would like to see some of the things that you're doing. I'll see if I can dig up some real examples.

MATTHIAS HUDOBNIK Matthias Hudobnik speaking for the record. So, two things, first of all, I think it looks very good. My first question is, is there also a plan

to maybe make a quiz after every chapter so you can just check if you understood, where say, for example, you have chapter one, and then you have one or two questions, you need to tick the box or so, and then you would test your knowledge a bit? And the second thing is also, it will be also hopefully made available on ICANN Learn, because I think it would be very good, so a broader audience could also make it and just learn from it.

JONATHAN ZUCK

Thanks. It's a great idea. I did have some quizzes in an earlier version of it, and thought that the jigsaw quiz encompassed that, but maybe it's better to have verbal quizzes, just quizzing the audience, especially in a live seminar, so I can revisit putting them back in. And we have talked about an ICANN Learn class. It wouldn't necessarily look just like this, but generally ICANN Learn classes look like textbooks from the '70s.

And I learned eventually it was because of Americans with Disabilities Act, and the need for them to be readable by screen readers. And I'm like, I'm dyslexic, so when you give me 30 pages of text, that affects my disability. But I think it would be worth doing, and so we should look into what something like this might look like on the ICANN Learn, for sure. It's a good suggestion. I don't know the order anymore, with the cards, so.

LAYAL JEBRAN

Layal Jabran here for the record. So, I saw you introduced MFAs, so awareness about MFAs. My question is, given that part of the MFA

is SMS authentication, which is very vulnerable, would you consider also including pass keys? So, talking about pass keys is really important. Thank you.

JONATHAN ZUCK I don't even know what pass keys you mean. You mean like the authenticator apps and things like that?

LAYAL JEBRAN Yeah.

JONATHAN ZUCK Maybe. I will say the tension here is trying to identify the audience that we're going after, and so we really want to focus. I know that at one extreme, Sébastien did like a trial run with some of the earlier versions with some elderly women, I guess in like a retirement community or something, and they found it overwhelming, right? And so, I don't know where to draw that line, but I'd be happy to talk with you guys about what simple messaging or examples might be worth including. Certainly, no objection, but it's about trying to be fit for purpose with the people we're reaching out to.

LAYAL JEBRAN Just to follow up on that. So, given that pass keys are being implemented by default now, for example, with Google.

JONATHAN ZUCK Right, for two-factor authentication and things like that.

LAYAL JEBRAN Yeah, because at some point they're just going to remove everything and go for pass keys.

JONATHAN ZUCK Okay. Yeah, did you want to…?

TARA WHALEN I guess I'll add on to Layal's point, because I completely agree with that. And I'm also very sympathetic to the whole matching it to the audience. The thing I'm always concerned about, and you probably are too, is the sort of telling people that the expectation is almost that they are able to recognize a URL as being the wrong URL. And the amount of effort that is put on the individual human being to sort of make the right call is, like, that that's really difficult. So, anything, like I said, the multi-factor, the pass keys, as much of pushing that, or if you have this option, or it won't fit for everything. Maybe that's a second level, but encouraging these things--

JONATHAN ZUCK I would suggest as a remediation.

TARA WHALEN Yes.

JONATHAN ZUCK Like you were saying, there was some compromise happening in the context of those things.

TARA WHALEN Oh, gosh, no. It's just that some of these things give it--

JONATHAN ZUCK And I was about to give up and just give up my money, I guess, at this point.

TARA WHALEN I mean, none of these are perfect, but it's more like the difficulty is saying, oh, we gave you all the information in a way, and it's all there, if you could just figure it out. But we know that it can be really difficult to make these judgments.

JONATHAN ZUCK It's true, yeah. In the '90s, it was something like 80% of passwords were not lost to hacking, but literally people calling on the phone and asking, what's your password? And people giving it to them. So, it is a high expectation.

BARRY LEIBA But on just finishing this, on fitting it into the audience, that the audience is already seeing requests from websites and apps and other services to switch to passkeys.

JONATHAN ZUCK So, encourage them to go ahead and do it.

BARRY LEIBA And explaining to them what they are is important.

JONATHAN ZUCK It's a good idea.

SÉBASTIEN BACHOLLET Sébastien Bachollet. I'm going to speak in French, if I may. Thank you very much. Sébastien here. And I used the first version of Jonathan's course in French in order to localize it in French and to find examples that I could use in my course and try to present it to older ladies, retirement-age ladies. And I understand that, and it's quite normal, it's your job to be very complete in what you present.

But we have to know how to present this course. What are the examples that you're going to take in each and every country? And it takes a lot of time. It's time-consuming. That's one point. So, can we have a presentation that is going to have several levels, several layers? We have different classes you go through, just like you do in school or in college. It's going to take a lot of work.

So Jonathan, first, thank you for doing this work. But let's not add too much on it. Let's use what we have and let's see what feedback we get after we use this course. It's not for specialists. It's not for experts. It's for people that absolutely need it. And I am deep in the countryside in France trying to explain that. It's quite complex and difficult. And when you try to explain what works on a

telephone, on a tablet, on a computer, what type of computer, what brand of computer, it's already quite a lot. And it takes time. So, let's take that into account. But it's great what we already have. Thank you.

JONATHAN ZUCK

Thanks, Sébastien. I think that's a good overall thought. I think with the clarification, we're just adding to a list of things to encourage them to take on when they're approached about them, essentially. They don't even need to learn the underlying technology of them or anything. And so, I think that's probably an easier one to add. I think there's plenty of other things that we might need to draw the line on. I don't have my participant list up here, so let me-- I've got Robert next. You have over 10 minutes. At 12 minutes, we'll bring him in. Go ahead, Jeff. Thanks.

JEFFREY BEDSER

Jeff Bedser. So, one of the areas that should be considered here is that a growing trend in the parties that mitigate the abuse is something called fake shops. And fake shops in their perception of the exact same outcome as a phish, but the delivery mechanism is a social media platform. And when I say fake shop, be very clear, it's one of the few times in the ICANN world where it means what it says. It's a fake shop. It's not a shop selling fake goods. It's a fake shop. It's designed to make you believe you're buying goods, but they're just going to steal your information and your credit card.

It's a very big growing trend. It's the exact same fraud as phishing. It's just a different delivery mechanism. So, it might be something to add here. If you see something, the price doesn't look right, and it's being delivered to you through a social media platform, and it takes you to a new domain, it's basically phishing you through a social media platform.

JONATHAN ZUCK: Well, we can really boil this down to one slide that just says, stop going online, right? I think that's where we are. It's scary out there. Oh, my God. Yeah, all right. Thank you.

NABIL BENAMAR: Nabil for the record. I just would like to emphasize here that with the introduction of AI, everything has been changed dramatically or drastically, especially the phishing attacks or phishing email attacks. We have just started discussing this topic in SSAC, and based on this, I have asked one of my students to prepare a survey paper on the existing approaches on combating this kinds of attacks. And we found a huge number of papers that have been published so far tackling this topic, meaning that this is an urgency. So, we need really to rethink our approach in combating the phishing attacks using AI. These are AI-generated email phishing attacks, and fortunately AI can also detect these attacks to some extent. Thank you.

JONATHAN ZUCK: Yeah. There's an arms race happening there definitely with AI. Robert, I think, is next.

ROBERT GUERRA: Sure. It's Robert Guerra from the SSAC. I think one thing I'm hearing is I'm hearing a lot about trying to improve the course, trying to do quizzes, and having different test markets. But one thing that's really important that I'm not hearing is that the need for this is more than ever. The environment that activists and others find themselves here in the US and in many other countries, the threats are much higher than ever. So don't wait to get it perfect. Get it out. Get it to people. Get it translated. There's an incredible need for that in many parts of the world. And I would just say, particularly phishing, particularly including new things, don't waste your time with one market. Just get it out because the need is there. So, that's my thought on that. Thank you.

JONATHAN ZUCK: Thanks, Robert. Hadia.

HADIA EL MINIAWI: Thank you. This is Hadia for the record. And I just raised my hand to comment on what Sébastien was saying. So, during COVID time, I did do a couple of webinars about online safety and online fraud, and it was in Arabic. I actually did include SMSs, and I also did include the two authentication factors in how to mitigate that or how to protect yourself. And the webinars were to a network or a group of nonprofessional women. Most of them were retired and, I

would say, 70+. And it was very well received, and they did understand what was actually presented to them, and they were very interested in knowing more.

So, the perception, I think, that if you're older and you don't really have a professional career, you won't be able to understand what's being presented, I think is not right, because if you're online, then you so much appreciate all the information that you can get in order to protect yourself online, or even through SMSs that you get. And also, it could include also phishing domains. Thank you.

JONATHAN ZUCK: Yeah, sure. Go ahead.

MATTHIAS HUDOBNIK: Matthias Hudobnik is speaking for the record. Just very quickly for everyone, there are really brilliant guidelines online from, for example, Privacy International, Tactical Tech, and also security security in a box. And there you can really check. So, they are for different audiences and also various things, so how to set up a password, how to use multi-factor authentication, use different email addresses, really kind of self-defense in the digital world. And I think it's very helpful. Also, for example, which plug-ins you should use in browsers that you don't have any advertisement, cookie tracking, whatsoever. So, that's also, we could also use some information from there, because it's heavily tested on a lot of people, and it's really to the point.

ADRIAN SCHMIDT

Adrian Schmidt for the record. A couple of things. One, in my day job, we all have a day job, unless you're happily retired. I'm an IT director for a nonprofit. We had a campaign that we were delaying, but this year we decided to go ahead and present the Cybersecurity Awareness Month. That was supposed to be in October. We did it one month late, but it was good. And we got very good recipients on the other end to get to there.

The other thing that bothers me, and this is-- That's only the first point is to support, let's get it out and let's get it to the people. The second one is how do we reach to the older generation? My dad passed away a month ago. He was 92. How can I help him from the technology to make sure that he doesn't get stolen funds and all that? We need to rethink, at the same time that we are preventing all this phishing, we need to rethink how we run the new internet.

And I see that as a problem from both sides. The older generation, that they don't understand that, oh, this looks like my bank. I will just call them. But the same happens in a different way to the younger generation, that they were born with technology, so they are trusting more than we, the older ones, that we saw all the evil there. So, we need to find innovative approaches that will not be government getting into there like we are seeing in different places in the world, where they, oh, we need to decrypt everything, and then you will be secure. We need to find a different way to build technology where the only weak link will be the person, and that's

my only defense. It bothers me very much. We need to build a more resilient technology at the same time. Thank you very much.

JONATHAN ZUCK: Yeah, I mean, social engineering has been the weakness the whole time along. Okay.

AMRITA CHOUDHURY: Thank you. Amrita for the record, I think, and it goes what Robert was saying, that phishing is, as an issue, the whole world is grappling. The only thing which we need to see is at ICANN, our remit is just domain names, but it is happening at the content phase. How do we get both of them together is the question. Because if you look at it, we may de-alienate it, but it's an issue which has to be looked at totality.

Yes, there is a lot of message, but if you're looking at developing countries, they may not be English-speaking, people may not be reading, so many times the video messages, et cetera, help. I know from India, because we are having huge financial frauds happening using all the phishing methods, et cetera. The regulator, the banking regulator, et cetera, are coming up with videos, et cetera, to teach, and more is required. Less is not more out here. So how can we make them more interactive so that people use?

And I agree that whatever we have, we should get it out and we can keep improving, but how do we also address the phishing aspects which comes from the content layer, not only at the domain name

layer, is something. We may wash our hands, but that's also important.

JONATHAN ZUCK

All true. It's a big problem. So, that's why we keep hounding the Contracted Party House on their end, and while you guys are advocating some technology-oriented solutions, and we're all trying to do what we can to contribute to mitigating this, but there's not going to be any perfect solution. I think we've gone through all the hands that are up and cards that are up. Oh, sorry, go ahead. Or I can go to Natálie Terčová.

NATÁLIE TERČOVÁ

Thank you. This is Natálie Terčová for the record. I just wanted to make a quick comment because I was focusing in the last four years as part of my doctoral work on actually digital skills and literacies of young people and children. And I'm very glad we've heard that elderly people are definitely a vulnerable group, but there is also this common and persistent myth that especially those born after the year 2000 are by default digital natives, and so they possess all the necessary skills they need to protect themselves, so we don't have to focus on them as much.

However, this is not really true, and we've been looking at this from my perspective on the European region with many countries in mind, and we saw that they tend to, when they self-report their skills, overestimate their knowledge because they probably feel ashamed that they don't know how to protect themselves, but if

you give them some performance tasks, you see that they still lack a lot of critical knowledge, and they also need help. So, I just wanted to highlight that also these are still here, and they need our help.And we see that also older people have the critical skills from the offline environment, and they're easily transferred to the online one, yet the younger ones, they don't have this, so we don't have to forget about them as well.

And just a fun fact, I tend to receive a lot of invitations for conferences, being an academic, and we usually had this little help, oh, you should look at how it is written. If there are mistakes, it's probably AI, but now it's flipped. So many of my colleagues, we were now rejecting some emails, thinking, oh, this is probably a scam because it looks terrible, but no, that was the poor human behind the computer who is not as advanced as the AI right now. So also, the mindset of how we can detect that something is a scam or is also a phishing attempt, these are changing rapidly, so this is another thing we should think about. Thank you.

JONATHAN ZUCK You're absolutely right. In my experience, young people don't even know how to boil an egg, so yeah, I wouldn't make any assumptions. I remember when it was all about Nigerian princes and things, and the emails were all full of grammatical errors, and what I heard at the time was that that was intentional. Because if you were educated enough to recognize the grammar errors and stuff, then you might be too much of a pain to deal with, and this is a volume game, and you're going to get rid of it anyway because of

the grammatical errors, and it's the people that miss the grammatical errors that are the most susceptible. So yeah, I mean, in all that, it's probably only made worse with the AI. Oh, without your card?

EMILIA ZALEWSKA-CZAJCZYŃSKA: Yeah, I forgot my card, apologies. But it's Emilia Zalewska-Czajczyńska.

JONATHAN ZUCK: Young people, right? That's what I'm saying.

EMILIA ZALEWSKA-CZAJCZYŃSKA: Not without flaws. Yeah, so I wanted to double on what Natalia has said and also to add about other vulnerable groups. Some European Union acts, for example, the recently adopted AI Act, but also some others, they name some groups that are especially vulnerable to different kinds of manipulation. These are elderly, these are kids, these are disabled people, and these are also people in the difficult economical, it's called social and economical situation, so different minorities.

So, I think what is also worth considering is because these are the groups usually talking about digital literacy. We talk about elderly people, we talk about children or young people, and there is also these groups like, for example, disabled people who are also vulnerable and also for them, their needs may be different and their needs in terms of capacity building may be different, not only

because of their disabilities, which may affect their capability, but also in terms how, for example, phishing and other kinds of cyber crimes, they may try to exploit their difficult situation. The same with people, for example, who had huge loans or who belong to minorities.

And also, what was mentioned here about AI, like AI really helps in collecting data on such people to target these people to do targeted attacks. For example, in Poland, a couple of years ago, this is a bit different story, but in some cases similar. So, there was a publication drafted by people who are flippers, who their profession is to flip flats, and they prepared some publications, like how you can easily sell your flat. And in this publication, there were some links. And if you clicked the link, for example, I want to sell one-bedroom flat or two-bedroom flat, if you clicked on this, your data were collected and your email address you had to insert to get the publication was sent to the person who released this publication.

So, thanks to that, they collected data of financially vulnerable people who may consider selling their flats because they have loans, they have debts, and target them with their offers to help them to sell these flats. So, AI makes it so much easier. We throw a lot of our data in the internet, so it's easy to collect and to decide who belongs to different vulnerable groups. So, I think it is also something to consider that this angle of, first of all, other groups that only those first that comes to our mind when we think about

vulnerable groups, but also in these new ways on how those people can be targeted. Thank you.

JONATHAN ZUCK: Well, thank you. This has been very depressing, but it's always good to talk this out. I think to Robert's admonition, I think we're going to try to push forward and start trying to use these things, see how people react to them, let them grow and evolve, and get different people, teach them in different environments, and see if we do in fact need to branch them out or something like that for different groups.

But at this point, I think we promise not to exclude anyone. So, we'll try to reach different people through different alliances and things. Like I said, I'm pretty excited about the libraries because I think they reach to a lot of groups that aren't always in our radar. So, we'll see how that goes. So, give us some good news about some of your latest work, since I think we're done with all of it on this topic. Thank you.

JEFFERY BEDSER: I think we're going to INFERMAL

JONATHAN ZUCK: Yeah.

JEFFREY BEDSER

Sorry, I don't think it's going to be good news, but it's going to facilitate some conversations. Hopefully we can move things forward. So, what I'd like to do is do a couple of slides just informing everyone on INFERMAL. So, it's a report put together by the OCTO office. It's a study done by data scientists on answering some key questions that have been asked for quite a time based on some assumptions about phishing in particular and DNS Abuse.

The conclusion of the report is that there's an important in economic incentives and proactive verification in these concentrations of where the abuses happen as far as in the parties that provision domains with registrars and registrars. But it does not offer solutions to these problems. It's basically validating something we've been talking about for the better part of 10 years is that do low prices facilitate, do bulk purchases of domains facilitate? And of course, the answers are based on the study, there are concentrations of the problem in volume in places where the prices are lower or the ease and ability to get domains faster and larger volumes exist.

So next slide please. So again, going through some of the key findings, yes, lower registration fees do correspond to 49% increase in malicious domains. Free services of course do. Discounts do. Stringent restrictions can reduce abuse. It basically adds more friction into the system to prevent ease of access to acquired domains for abusive purposes. API access does account for a 401% rise in malicious domains, but there are some caveats to that based on certain types of technical abuses. And the

verification practices can again be a friction as a proactive measure to slow down on the registration of domains for abuse.

Next slide please. Reactive measures, mitigation times. This is something, one of the findings that we'll discuss a bit in the talking points that I'll bring up toward the end, but rarely except for of course with spear phishing, which is a topic that Jonathan did show us all, is there one victim targeted for a phish? So how many victims can there be within a second if there's a mass distribution versus how many within 10 seconds versus how many within 48 hours, that measurement in question. Registrar and TLD preferences, of course there's a concentration of abuses in certain TLDs and based on business practices, lower prices and free services.

Next slide please. So, pricing and ease of access. The key points are basically that, here look, it's economics. People will go to the place where the prices are lower. That's why particularly in North America with the big box stores, the Walmarts, the Targets, et cetera, they grew quickly and had a lot of business because they offered a lot of lower prices and they offered the ability to buy larger amounts. So, I don't think it's a surprise to anyone in this room that the concentration is going to be where the prices are lower.

However, you saw the numbers on the previous slide deck that Jonathan provided, and I've seen numbers from 1 trillion to 10 trillion in cybercrime losses related to domains, and that's really up for debate, a debate I'm not going to have right now, because 1 trillion is a number I can't conceive anyway, so you add a zero to

that, sure, it's bad. But at what price? With one domain, the average loss per victim globally is 138. It doesn't look great for the US. In the US, the average loss is, oh, 3,520. Apparently, we have more money and we're stupider.

I'm not really sure how that works, Ram. But if that's the amount of money that a criminal makes on a domain, at what price are they not going to buy a domain for a criminal purpose? We're talking about cybercrime being one of the largest economies on the planet. It's like the second-highest GDP, or third-highest GDP, depending on whether it's 10 trillion or 1 trillion. So, the reality of price, concentration of low prices is where it's going to concentrate, I think this is a fact that we can all acknowledge, but I'm not sure it's something without doing price fixing at a very high price per domain, which I don't know how that would work either. I don't think there's a solution around pricing, because it's always going to go to the bottom and there's always going to be a bottom price.

Next slide, please. Verification processes. There are quite a few country code TLDs that have very strict verification processes. But for the most part, they are manual, because the ability to create digital identities that not only completely can create a fake person, a not real person, but can be used to use your identity to create an ID that has someone else's photo on it that looks very good. And AI-generated ones are significantly better than it used to be when they had to try and generate their own, because they don't have to know what state of Pennsylvania driver's license looks like in some

other country. They can go find those details and create it with AI and have a driver's license that looks like it's my driver's license.

So better verification processes is something that is at risk just based on the way technology keeps moving. Yes, you can do it, and you can basically insist that a human has to speak to a human each time a new domain is registered. But I think the practicality of that volume is a question for anybody's practical use of the system.

Rates of detection from delegation to mitigation, is that a valid measure? And I would say it is. I think that the analogy I like to use when it comes to DNS Abuse is that all the public reports you see that are generated by all the parties that put up those annual reports and quarterly reports on what domain abuse volumes look like from NetBeacon, from ICANN, from InterRail, from Spamhaus, they're looking at publicly available data, which to me is the top of the iceberg.

Every one of the parties being targeted by these types of abuses has abuses all day long that they are mitigating that never show up on those lists. And the take on top of that measure is that reports of abuse are because someone detected it and someone reported it. Now, we can all guess that how many of us here have deleted a phishing email and didn't report it? Everyone in the room. If you haven't, tell me your secret, please.

So, the vast volume is unreported. We don't see those numbers. So, to me, it's about time from delegation to mitigation is the key factor. So, if you can as quickly detect it as possible between delegation and then basically mitigate it within seconds, so maybe,

yeah, there are 10 victims in that two-second period or 10-second period, but at the same time on a reducing victimization, which is really the goal of taking on this target, especially within the training with the ALAC, et cetera, it's about the availability of the domain and getting it killed less than trying to stop people from being able to get them for crime because there's a financial incentive for the criminals to get them, and they'll always find a way to get them. We've got to figure out how to best get them reported, detected, so they can be killed.

And then, yeah, I guess the other question, of course, being measuring the number of victims per domain would be a more helpful metric than the number of domains reported. So, we can understand the size, the cost of the losses and where the victims are.

Next slide, please. So, one of the points about the measures before, there was a 401% increase when there's an API available for the registration of domains. However, DGAs, which are digitally generated algorithmic domains where they get thousands of them to spread malware, create a botnet, et cetera, one or two registrations for a DGA could throw off the entire volume for an API. So, at what level is appropriate to restrict the buying of a large number of domains?

I know that in a corporate sense, when someone's launching a new brand or a new product, they will try and buy a single brand name across a large number of TLDs, and it could be several thousand.

Well, so how do you tell that from a criminal one? We have to have better processes around that.

Next slide, please. Okay. So, that was the last slide. So, those are the talking points. I think these are all the type of questions that we should be focusing on that Domain Metrica has confirmed something in the fact that we know that there's a concentration, bluntly, around the economic incentive of getting something at the lowest price. We also know that the economic incentives for the cyber criminals far, far, far outpace the cost of the system, but we also know that to jack up the prices enough to keep it out of the hands of cyber criminals means all the people that ALAC represents will not be able to afford domains because it will be far too high.

So, we need to look for solutions bluntly around reporting, detecting, and then speed of mitigation to avoid victimization so that the cyber criminals realize that there is such a small window in which they can do the abuse that it's not economically valid for them to use this methodology to victimize people.

RAM MOHAN Robert is in the queue and then Satish. Robert? No? Okay. Satish?

SATISH BABU Thanks, Ram. Actually, this is from the previous section, but I think it's still relevant. Just this month, earlier this month, the Central Bank in India issued a circular that introduces two exclusive subdomains, .bank.in and .fin.in, which the banks and financial institutions in India are mandated to use. So, I'm just mentioning

it. I'm not sure how successful this is going to be, but it does provide a control point where people cannot do large numbers of domain registrations. Thanks.

RAM MOHAN Thank you, Satish. Jonathan?

JONATHAN ZUCK Yeah, I guess I was going to say something similar, is that there does seem to be that in domains with more restrictions associated with them that there's less concentration of abuse. And so, maybe it's about trying to push, especially, and the GAC has been on about this for some time, push heavily regulated industries, doctors, and lawyers, financial institutions into restricted TLDs might be helped so that then what you're teaching people is to look for this small subset of domains and not be responsive to others.

The conversation I'd love to have generally is what, if anything, do you think we should be doing in encouraging the content of parties, generally, maybe the registrars in particular, that doesn't seem completely irrational but is worthy of some negotiation, some discussion with them about what they might be doing that they're not. Is it verification, is there something that is worth doing, or is it-- Because otherwise the conversation becomes just one of hope as opposed to action, I guess. So, that's my question.

JEFFREY BEDSER

So, I think that one of the hurdles, and this was something that came out of SAC 115, which is about interoperability and DNS Abuse management, is that the need for the contracted parties to have to verify every report of a harm to be able to act upon it is a friction point. Wherein that's one of the reasons why the new obligations say a well-evidenced report of must be acted upon, which means if the reporter sends the evidence, the action is much less friction to have it actioned. Because if you need to have a person investigate every phish that comes and reports to you, at the volumes we're talking about, you're looking at backlogs of weeks and months even for teams of a dozen people working on this.

So, I think one of the keys, I think, and this actually might be very interesting to add to the educational component of the previous session is not just how to not be phished and what a phish is, here's how you report a phish. Let's get the process out there to get people to report it because it was, bluntly, six, seven years ago, you reported it, nothing happened. Some parties would, some parties wouldn't, but also because there's so much effort into validating it, you stop reporting it because nothing ever happened. That's not the environment we live in now, at least in the gTLD space, where there's an obligation to take that.

So, if we can get an educational component in about this is not only how you not get victimized, but when you see it, this is how you can report it. And we've got mechanisms like NetBeacon ready to roll

that actually enforce the evidencing standards so when it's reported, all the evidence is there to get it mitigated.

JONATHAN ZUCK: We're cognizant of those and we've done some outreach to our own community about those tools and things. My one frustration with the NetBeacon tool is that it requires getting the header of the email to be part of the report process, which I think is something that excludes most people that might otherwise be reporting. It would be great if there was a tool that was just based on forwarding or something like that where the header comes along with it because telling people how to get the header to an email is worse than anything that's in this vision course, I think.

JEFFREY BEDSER: We can solve for that because basically CleanDNS donates the software to NetBeacon for that purpose and if that is a friction point, an actual phishing evidencing package does not require that. If it's requiring that for the submission, that's a fixable point. I'll talk to Graeme. We'll get that fixed.

RAM MOHAN: Olivier?

OLIVIER CREPIN-LEBLOND: Yeah, thanks very much, Ram.

JEFFERY BEDSER: I think there might be an echo somewhere.

OLIVIER CREPIN-LEBLOND: Hello again? Okay, that's better. Yeah, thank you very much. Olivier Crepin-Leblond speaking. I'm looking here at the INFERMAL report. That was released in November last year, if my understanding is correct. We have a new administration in the US and the world has pretty much, I think, changed since then in that there's a lot of things changing and I'm seeing this.

What's happened since then? It's been four months. Is there any action item, anything that will come out of this rather than having the old, oh, let's educate people, let's continue the same way we've gone so far? Is there going to be a disruption in this space? And are we likely to actually take some stronger stance regarding these issues? Or are we set to continue in saying, oh, we're doomed, we're in trouble, goodness, or let's do some more reports about how bad this is? And I'm being just to see what we can do.

RAM MOHAN: If you could just go back to the previous slides that provides the conclusions and, Jeff, if you want to take that.

JEFFREY BEDSER: Yeah. You're not wrong. And in a public forum, I'm probably not going to respond to at least 50% of that. We can have a conversation privately about that. But at the same time, as I said, the biggest problem we have is this problem is we're dealing with the tip of the iceberg and we need to get the idea-- The contractor parties have gone to the very big step of volunteering to do more

and be required to act. But that is only going to be facilitated by getting more reports in their hands to act that are well evidenced.

So, I think that I don't know of good mechanisms that exist today to detect the abuse through automation. It's basically relying on victims seeing it and reporting it. And we need to be better than that. We need to figure out how to get from you're waiting for a victim because it means there already have been losses to stop it and stop the concept that-- What's the minority report term? Pre-crime. That's pre-crime. You're trying to stop something before it happened.

But criminals do use the same infrastructure over and over again because infrastructure is expensive. And you can look at patterns and determine this domain is most likely going to be used for bad. And you can put in proactive frictions at least to prevent the delegation of that domain until a better know your customer process that can be managed a few wise can be done. So, yeah, I think that's I agree. My frustration is the constant reports on the same five data sources over and over again and how bad things are and how things have gone up and down when we're only measuring the top part of the iceberg. That scares me because I know how much bigger the iceberg is.

RAM MOHAN Alan.

ALAN GREENBERG

Thank you. Alan Greenberg speaking. I got a phishing SMS the other day and I actually reported it. And a couple of days later it was still active. And I happened to be on the same flight as Graeme the other day. And I asked him how quickly typically people respond. He said, "Well, some risk registers very quickly and some not at all." So, yes, there are obligations, but they don't necessarily honor them.

I think our only choice at this point is to look for the low-hanging fruit. And bulk registrations is one of them. There's clearly established know-your-customer processes that can work, that can say who is allowed to use the API and who isn't. And you have to at least ask for it first and then justify it. And then if you have domains taken down for abuse, you can no longer use it. Some of these things are easy to implement. All we have to do is somehow get them implemented. That part isn't easy. Thank you.

RAM MOHAN

Alan, I think that's exactly right. The part of it is inside of our environment to perhaps the first thing to do is to publish some level of best practices. What are sensible practices that can then be considered inside of the policy development environment? Because if you started up a PDP on something like this, by the time it comes up with the result, all the recommendations that it recommended would be obsolete because of obvious reasons.

As Jeff said, more and more parties in this environment are stepping up to try and mitigate and to reduce the incidence of these kinds of problems. It's not uniform. But I think that what we ought

to be looking at, perhaps as a measure, is not uniformity, but trying to get to a tipping point, trying to get enough of all the parties that are involved to conform. That's on the one side.

On the other side, I think, and this is something ALAC and SSAC is happy to collaborate with you on this, is to really get much more education on not only how do you recognize you're being phished, you're being targeted, but what can you do with it, how do you report it, how do you share it, send it onwards, et cetera. And having that information then results in a data stream that we can then look at and then we can go and point to those who are expected to act on it and say you had an incidence of so many reports coming your way. What was your response to it? Then you have something that we can act on. Something we can apply some pressure on. Right now, it's a little bit more of do your moral duty. And that often conflicts with do your economic duty.

ALAN GREEBERG If I may, unfortunately, do your economic duty often is let's get the revenue in and not worry about the impact of it. And some of these discussions would be more interesting if we had candid Compliance people here in the same room who would be willing to actually interact with us, not just quote the party lines.

JEFFREY BEDSER One of the points on the economic point is that the majority of the metrics I've seen that neither registering or registrar makes any money on the first year of registration. All the costs go into that.

Usually, it's underwater. And as soon as they spent any time or money on abuse, they've lost money on that domain, if not more money on the domain.

The money is made on renewals and almost all abusive domains, with some exceptions that are the outliers we're talking about. Don't get past 365. At 364 days there, they're gone. They didn't get paid. They're not going again. So, the economic incentives are more about. And also, this are getting charged back frauds because credit card fraud was done as well. There's economic incentives to be better, less than there are to not be good unless it's growth for growth's sake versus growth for economic sake.

And one of the things I just want to remind everybody, this probably is preaching to the choir, as they say, the cyber criminals are looking at ways to get around all this and anything we talk about in a public forum here. They're watching this stuff because, look, what are these guys, what are they going to do? I know that, for example, there are registrars that have a problem with legitimate customers buying accounts, I mean, creating accounts, funding accounts, buying domains and then selling the entire account and with the credentials to someone else who uses it for crime.

How is a registrar supposed to catch that? Right. How are you supposed to get around the fact that they know they can get those domains and get around to know your customers by basically buying and selling accounts? It's almost like an unauthorized reseller. So, that's the point I keep making is that it's not about restricting access to the domains. It's about figuring out how to

	catch them and stop it versus trying to put restrictions in place that the cyber criminals are usually 5 to 10 steps in front of us, figuring out how to get around whatever we're coming up with the block.
JONATHAN ZUCK	The promo is right.
JEFFREY BEDSER	Well-named.
RAM MOHAN	Okay. It's not all doom and gloom.
JONATHAN ZUCK	We're waiting for the good stuff.
RAM MOHAN	This is the silver linings part of it. So, this part is to really initiate a dialogue with you, but also to share with you the five keystone areas that the SSAC is focused on. I used to call these steady state topics and then someone told me that it abbreviates poorly. So, we are now calling this keystone topics. So, on these five pieces we've engaged with you in many ways, primarily on the first one on DNS Abuse. That has direct impact on end users. It it's very expressible and tangible. And what we want to do is continue to work with you in a safer cyber. It doesn't stop with this first campaign. What we've done here together, I think, is

excellent as a start. But we have another 125 documents that be written with the findings and with recommendations and things like that, that that we think could also-- Not all 125 of them, but many of them have real life practical measures where some of them are aimed about the IANA transition, which I don't know that end users care about anymore.

We want to work with you on those aspects. What we need from you to ask from you is, and we can have a curated session with you, but which of those main topics that we have, which of those have the most amount of resonance and need for the audiences you're aiming at. Because it's one thing to have a plethora of information, but the real the real goal is to take it and shape it so that that information can actually be used in a good way. So, that's if

On DNS Abuse in particular we have I suspect, Jonathan, we have. At least 30, 40 documents that we've written in that area. There's a deep vein that is available to mine on that one. On New gTLDs. Just to refresh your memories we've been involved in looking at and opining and commenting and providing advice on new gTLDs for a long time. The most recent thing that we've done is name collision analysis and a set of recommendations on how to avoid, when New gTLDs are introduced, how to avoid not just confusion, but actual collision with names that are all that are already being resolved, that are already being asked for today on the Internet.

So, a good example of it in the prior round was applicants who applied for .home or .corp or .mail. They applied for it. And what they didn't realize was that those three TLDs names had already

been used in on the Internet for many years, sometimes a few decades prior. So, there was a lot of traffic already flowing on the Internet that was using a .home moniker or a .corp moniker. There's lots of we've written about it. There's lots of work in it. But we've provided to ICANN and the Board some clear guidelines and recommendations on how to avoid or at least mitigate such collisions in this Next Round.

On DNSSEC, it's been a quite a while. It's been almost two decades now since its implementation has rolled out. And we're starting to look at in all of this time that has transpired and the operational execution that has happened, what are the observations we can make. One of the observations anecdotally is or even empirically is that some level of extra fragility seems to have been introduced when you're trying to roll over DNSSEC keys. And that has resulted in TLDs across the board, TLDs small TLDs large TLDs by well-resourced operators, TLDs by ill-resourced operators to have problems when those things happen. So, we're in the process of looking at a charter for some work in this area. We haven't actually begun the work, but that's where we would like to go.

On alternative namespaces and inside of this ICANN world that's primarily expressed as the many initiatives that are exposed, that are available about blockchain namespaces and the integration interaction with the DNS namespace. So, we've just commissioned a work party to look at what would responsible integration of these workspaces into the DNS. What would it look like? What are characteristics? If you were to integrate these namespaces into the DNS namespace, how would you do it in a responsible way so that

security and stability parameters are not affected in a negative way? So, we've just begun the work on that and we'll report back to you on what that means.

The thing to underline on that is that inside of the SSAC, the approach with respect to blockchain as an example and names in the blockchain or other spaces is not a reflexive one. It's not, oh, it's bad, and therefore you have to block it. We rarely look at what are the motivations behind somebody coming up with some new innovation. We mostly focus on there are new innovations, new developments happening. How do they impinge on the integrity and the stability and the security of the namespace that we all depend upon? So that's our clear focus. So, there's work that's beginning in that area.

And finally, Olivier, you were talking about a couple of changes that are happening in the world. And we don't focus too much on the geopolitics of these things. However, we pay attention to the SSR aspects. And our general approach in that area is to try and provide practical, actual, real-life clue. How does it actually work? How does a DNS actually work? If you are a policymaker or a regulator who thinks, oh, in the interest of national security, I'm going to pass a law that says all here is how DNS blocking should happen.

Our approach on that is not to opine on whether blocking is by itself good or bad, but instead to provide clarity on here are the potential unintended consequences that may come if you take a hammer to a thumbtack. So, that's generally our approach. We're tracking. I was just informed yesterday that apparently there is some work

that is advancing in the European Union, in light of recent developments, about some failover on DNS resolvers to force some a failover to European DNS resolvers. And I look at that and I say, wow, that's not engineering. That is real-life hallucination.

I wouldn't say this to a policymaker, of course, but we would probably say provide the technical details behind how resolution actually works and things like that. So, this part is to really say that the SSAC in general consists of complete skeptics who are optimistic about where the future should be going, could be going, but are also quite realistic about the fact that there are lots of forces, lots of folks who look to benefit from a base culture that says you can trust the other side of a transaction because that was the core culture that began all of this.

So, the members of the SSAC in general have that same mindset while also realizing that that's exactly what folks on the other side are looking to compromise, corrupt, erode, and degrade. So, that's the high level of the main areas that we're looking at. And I open it up for other SSAC colleagues or for ALAC colleagues.

JONATHAN ZUCK Unfortunately, we've reached the end of our time. We always have such good conversation with you. I think we need to not wait until the next ICANN meeting to continue some of these conversations. Maybe we'll put together a small team to look at some of the matchups, as you say, where we might see an end user, something

that connects with our remit a little bit, and how we might be helpful to getting some of these out to a broader audience.

Because right now, we've hit the end. We've got to let the interpreters take breaks and things like that. But let's commit to not waiting three months or whatever it is. I guess the next meeting comes in like 14 days, right? But let's meet and get on a Zoom and take through some of these things one by one and really tackle them. We really appreciate you guys coming to visit us every time. But it never seems like enough time. So, let's do more of it, because I think we have so much in common in terms of our worldview and things. And let's keep at it. So, thank you very much for everyone. And I'm sorry for everybody who had a card up. We'll figure it out.

RAM MOHAN Thank you.

JONATHAN ZUCK Thank you to the interpreters.

[END OF TRANSCRIPTION]