BRENDA BREWER: Good morning, good afternoon, good evening. Welcome to the Not-for-Profit Operational Concerns webinar number five on the 31st of March 2021 at 14:00 UTC.

Today's webinar is recorded. Kindly have your phones and microphones on mute until questions are taken. I will turn this webinar over to Adam Peake. Adam, please begin.

ADAM PEAKE: Thank you very much. Thank you, Brenda. Hello everybody. Adam Peake speaking. I work for Global Stakeholder Engagement. Caleb, I believe you're the representative from the NPOC leadership today, so if you'd like to make an introduction, pass it back to me and then we will kick off the webinar. Thank you. Over to you, Caleb.

CALEB OGUNDELE: Thank you very much, Adam, and thank you to all ICANN staff for all the good work that you guys have been doing. We are very grateful for putting in so much to help us engage with our members.

My name is Caleb Ogundele, I'm the membership chair of NPOC, and we are really glad to have everyone join us for this fifth webinar series that we're having. The whole idea is to see that our members have a lot of knowledge based on what we do and for them to have that knowledge base as something they can use to engage actively.

***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.***

So on that note, on behalf of the NPOC chair, Raoul Plommer, I'd like to welcome everyone and I'd like to also welcome especially Siranush who's also joining us, and every other member that is on the call. Thank you, and over to you, Adam. Thank you.

ADAM PEAKE: Thank you, Caleb. And yes, welcome, Siranush. Lovely to see you here. So, yes, as Caleb mentioned, we're running through this series of webinars. We're on number five today. So far, we've covered issues that the NPOC leadership designing this program thought would be sort of the definition of what operational concerns are.

So far, we've walked through issues such as registrant rights and responsibilities, how to register domain names and what's involved in the management and renewing of domain names. We've looked at rights protection mechanisms, protecting names in various ways. We've spoken about policy development processes, which of course is at the heart of the Generic Names Supporting Organization and the work that NPOC does as a community there.

And in a moment, we will begin looking at issues around protecting and securing domain names, and this will be the subject both today as you can see on the introductory slide here and for this webinar and the next one, we'll be talking about both protecting and securing domain names but also securing domain names in terms of operations, so what an NGO that's providing DNS for its members and for its communities needs to know about in this sort of operational concerns context.

With that, I think we can move over and first presenter is going to be Brian Gutterman, and then we'll move on to David Huberman. Welcome, David. David works for the office of the CTO's team, and so will cover some of the technical and operational security concerns today. So, Brian, over to you.

BRIAN GUTTERMAN: Thank you, Adam. Good morning, good afternoon, good evening to everyone who's here live today, and of course, hello to everybody who may be listening to this recording sometime in the future. Thanks for joining us here. We hope you find this content useful. I'll note we just started coming off of a very busy ICANN 70. We've been on a more than three-week break. I hope everybody had a good ICANN meeting. Lots of interesting topics out there and I know NPOC members and the broader community was very engaged, so the Org and the Board certainly appreciate that.

So, where are we today? With the series, as Adam said, this is webinar number five of seven for now, and we are moving into sort of more of a security-focused part of the series. So today, I will be sort of giving the basics and introductory talk about protecting and securing domain names, and then I'll pass it on to my colleague, David Huberman who we are privileged to have with us today. He's an expert and a great resource. So, thanks to David for being here with us today. Next slide, please.

So this is where we are, so five, six and seven, this is sort of previewing where we're going to go. We expect webinar seven to have plenty of time to sort of wrap up and talk about where we are, do some additional Q&A and think about next steps for NPOC. Next slide, please.

Without further ado, I'll go into this next portion of the series, protecting and securing domain names. So a reminder for everyone, whether you are a domain name holder, a registrar or not, but thinking about how also NPOC members can really do some good outreach and education to nonprofits, which is again an important part of NPOC's mission to help nonprofits treat and remind them that their domain names—which is part of their brand, part of their presence online and in the world, domain names are valuable assets.

So even if the cost of registering a domain name might be minimal to some compared to the rest of their expenditures on their nonprofit organization, they are indeed quite valuable assets, and the services connected to them like the websites and e-mails, of course, they become essential to their professional and personal lives of a registrant, of the organization, whatever it may be. So whether they use domain names for online commerce or simply to communicate with family and friends, domain names are indeed valuable assets and should be managed with care. So we urge everybody to frame their mindsets remembering that they are valuable assets and hence need to be protected as such. Next slide, please.

So, let's start off with some best practices. Again, some of this, the slides may be a bit text heavy. We want this to be a resource that lasts a long time, however, and we hope you can use these slides not only for yourselves, for your friends who are registrants, but for nonprofits and organizations who NPOC believes that this information is important, which it is.

So, some best practices to help prevent hijacking or unauthorized transfers of domain names. Number one, register with an e-mail address that is not connected to your domain name. So when you register, as we've talked about before, you'll be asked to provide some basic contact information, including an e-mail address where your registrar can contact you. This information, some of it may be public. It’s best to use an e-mail address that is not associated with the domain name you're registering. For instance, if your domain name is example.com, a best practice is to use an address that is not user@example.com. Why is that? If your domain name is hijacked—which can happen, unfortunately—by someone who has gained access to your account with the registrar, that person may try to change the information. But if you use an e-mail address that is not associated with your domain name, something separate, you'll be able to provide that e-mail address as evidence to the registrar when they're investigating what happened. So that is our first best practice. I see some people are coming into the room. That’s great. Next slide, please.

Continuing with these best practices, strong unique passwords. Again, to those here today or watching this recording who are more from the cybersecurity world or more security-minded or who follow the SSAC work, apologies, but these are all sort of basic best practices that we need to constantly remind ourselves of.

So protect your domain name from cybercriminals by creating a strong and unique password. Online services are compromised frequently, making usernames and passwords available to criminals who may attempt to hijack your domain name using the information you provide for other accounts. So avoid this by creating a strong password that you use exclusively for your domain name account. Don’t use the same one that you use for something else in your life. Make this unique for your domain name. Don’t share it. You're responsible for the security of your domain name. You should never give anyone the login information to your online accounts. This includes webhosting providers, web designers as well as friends and colleauges. It is not recommended that you list website designers, hosting providers or any other third parties as the registrants of your domain names. Another tip, if you choose to do so, seek legal advice as to contractual obligations that third parties should adhere to with regards to the administration of your domain name. Next slide, please.

More best practices. So, ask about multi-step authentication. Some registrars offer registrants, domain name holders, the ability to implement a multi-step authentication when accessing your account. This provides added protection by requiring a unique security code in addition to your username and password to access online accounts. Refer to the terms of your registration agreement to see if multi-step authentication is available. So this is another piece of what we've talked about in earlier webinars about what to do before you register a domain name. Really do your homework about what services are offered by a registrar and what you need to do besides getting the domain name to get your online presence up and running.

I don’t see any questions in the chat. Moving on, check the e-mail accounts associated with your domain name frequently. Don’t let these—even if you're not using it, individually or as an organization, as a nonprofit for example, day to day, continue checking the e-mail accounts associated with your domain name frequently because whatever e-mail address or addresses you provide, you must be sure they're active and that you check them.

Keep your contact information up to date because you may be getting important notifications about renewals from your registrar to that e-mail address. If you use a privacy or proxy service, this is particularly important. Consider leaving your name as the registrant of record in the contact information. this can serve as another piece of evidence to your registrar that you were the registered name holder of the domain name, should something go wrong. Next slide, please.

Ask your registrar to put a transfer lock on your domain name. This is something you can request from your registrar, a transfer lock. Putting this lock on your domain name is not a failsafe way to guard against unauthorized transfers or hijacking of your domain name, but it could be another layer of security. So all these best practices, they're not going to be failsafe, but each one, you can implement practically will help protect your domain name. So each registrar has a different way of implementing the transfer lock. Some require two-factor authentication to remove the lock. Some simply require authorization from the registrant. Check with your registrar about their policies regarding transfer lock and decide whether it is a service that’s right for you.

This actually reminds me of—some of you may have participated in a few sessions at ICANN 70 which are relevant here, so I'll mention them. The community is about to undertake a review of the transfer policy.

Something that’s very important in this review is that the interests and perspectives of the registrant, the domain name holders, are there when reviewing this holistically. So every part of the community of course has a hand in this, but it’s important that the perspective of the registrant is also represented in that. I know some colleauges from NCSG are involved in that already, and I would encourage you to do this because one of the things that’s happening in this PDP, in this review is a review of things like the transfer lock. Are they working, are they not? In regards to the transfer policy. So here's a PSA to get involved and to have a look at this transfer policy review and see maybe if NPOC has anything to say about it. So that’s a bit of an aside, but I wanted to put that out there because it’s relevant here, and we've talked about transfers before.

Moving on to continue with these best practices, be smart about your online behavior. We all get lazy. Be cautious with the links you click in e-mails, with the attachments you open, with the websites you visit. These are unfortunately sometimes means that criminals can use to steal your username and password. Unfortunately, we can all be guilty of this. We’re tired, we've been working all day. But stay vigilant. Next slide, please., Brenda.

Okay, a bit here about phishing attacks and how to protect yourself. Next slide, please. So, what is a phishing attack? It’s a type of fraud that cybercriminals utilize to lure others online, including domain name holders, into doing what the criminals want them to do. Phishing may result in others voluntarily giving away their username and password or clicking a link that will lead to their devices being infected with Malware, which is software that when installed performs unwanted or malicious activity. Sure you’ve heard of phishing scams before. If an attacker can gain access to a registrant’s private domain name registration information and passwords, they can potentially redirect a domain to wherever they like. As such, it’s immensely important that you take note of any suspicious or unsolicited e-mails. So again, stay vigilant, read every email closely, beware of these sorts of attacks. Next slide, please.

So for example, these sorts of phishing e-mails may claim that your domain name registration needs to be renewed and that you might need to pay some sort of fee to get it back. They use deceptive techniques such as forging a trusted sender’s address or domain or using a similar or lookalike domain. Phishing messages typically ask for the reader to reply, call a phone number, click a link or open an attached e-mail or file which results in stealing personal information or gaining some other advantage over the victims.

Sometimes phishing e-mails aimed at registrants unfortunately may appear to come from ICANN. So ICANN hears about these phishing scams from time to time. They can even use ICANN’s branding or logo or sender e-mail addresses. It’s important to know that ICANN does not send e-mails directly to domain name holders about managing their domain names—that is not our role—and never requests payments or fees from registrants, domain name holders. Really good thing to note here. Next slide, please.

Thank you. So just a few more tips. I've already gone over some of this. Carefully review every e-mail you receive. Phishing e-mails and websites often mirror familiar visuals. Like I said, branding, logos of the organization and appear—so they try to be deceptive in the way that they deliver these messages. Again, any e-mail or webpage from ICANN that offers domain name renewals or registration services, these are not real. ICANN Org does not process renewals or send WDRP notices. So, important to remember. Next slide, please.

And again, this is all information that if you personally today or if rue watching the recording, you may know all these things, or you may not be the registrant of record. This is information we want to really get out to the world to nonprofit organizations who have domain names they use. These are all best practices that we want to disseminate. So we count on our engaged community members to spread these messages.

Continuing on here, e-mail attachments may contain malware, hyperlinks may direct you to malicious websites or forms, never enter your password into a page you arrived at by following a link in an e-mail. Again, phishing e-mails often contain a false sense of urgency. "Oh, you've got to do this so fast, just pay me a little bit of money and we'll handle this for you." You see any of these signs, take a step back and contact your registrar. Next slide, please.

Again, be suspicious of any e-mail that offers domain name management services from ICANN. We do not send—as in ICANN—WDRP notices, registration data verification requests, domain name expiration reminders, etc. Contact your registrar—be vigilant, be safe, directly—for any concerns about the status of your domain name. Next slide, please.

We recommend using ICANN accredited registrars to register and manage your domain names. This is something we talked about, again, in the portion of the series when we talked about things to think about before you register domain names. If you're not entirely comfortable with a registrar after you register a domain name with them, you can and should consider transferring your domain name to a registrar that you trust.

Use TLS, transport layer security, HTTPS when you access your domain name registration account to prevent someone intercepting your communication with your registrar. Be proactive. If there's any sort of main takeaway that we want you to have about this, be proactive as registrants, as domain name holders. You are important players in combating DNS abuse, a topic we talked about a lot at ICANN 70 and past ICANN meetings. We always encourage you to be vigilant and proactive in securely and responsibly managing your domain name. Next slide, please.

So this is my last slide before I pass it on to David. I will introduce this topic of DNSSEC, and then I'll pass it on to my colleague. Another step you can take to protect your domain name and contribute to the overall security of the DNS is by DNSSEC signing all the data associated with your domain name. Domain name system security extensions, DNSSEC reduce the chances an attacker will be able to substitute their answers in response to DNS queries by creating digital signatures over your domain name zone data, clients looking up your domain names can verify the information they receive is what you had placed in the zone.

This is great. We have a lot of participants joining. Many DNS software packages and registration systems have tools that automate DNSSEC signing. Check to ensure that DNSSEC signing is enabled in your DNS software and at your registrar and that your registrar has the necessary information to help establish trust in the information that's signed. And with that, I will pass it on to David. Thank you very much. Again, we encourage you to use the chat to talk to one another and to ask any questions. I apologize that I seem to have had some shadows on my face. The sun is coming up here, and I can't help it. David, without further ado. Next slide, please, and pass it on to David. Thank you.

DAVID HUBERMAN: Hi everybody. Brian, I thought that was great. The longer you talked, the more the sun shined. Hello everyone. I am David Huberman, I work in the office of the CTO here at ICANN. Next slide, please. So when you open up your web browser and you go to a website—maybe you're going to Facebook, maybe you're going to ICANN.org where you're going to log into your ICANN account, or maybe you're going to your bank—wait, let's talk about that.

Maybe you're going to your bank. When you go to your bank in your web browser and you type the bank's URL, www.bank.whatever, and the home page shows up, now you have to log in. you have to put your username and your password for your bank credentials. When you do that, how do you know that the website that you're entering your banking credentials into is actually your bank?

I ask this question a lot, and I ask this question sometimes to highly technical audiences, to engineers who just assume they know how everything works. And they come up with a lot of interesting answers. The most common answer, the thing that gives people the most confidence that the website they're looking at on their browser right now, the website they're going to enter their username and password into is the correct website, is because the cookies are set and there is a username and password stored in a cookie that enters into the website. That gives people a lot of confidence.

But it shouldn't, because you don't know that the domain name information being sent is the actual domain name information that was supposed to be sent, the information that the zone owner, the domain owner, the bank actually put into the DNS.

And the real answer to my question to you, of how do you know you're really at your bank's website, is you don't. There's pretty much nothing you can do, there's nothing any of us can do as end users to get real assurance that when we go to a website, we log in, we've actually logged into where we intended to.

The way we've built this Internet over the last basically four decades is the DNS just has to work. We really on it to work. We assume it works. Every end user who uses the Internet assumes the DNS works. That's because most of them don't even know what the DNS is. But you, my friends, and we, we all know what the DNS is and we know how it works, and there's nothing we can do either. We just assume it works every time we use it. Next slide, please.

So the technologists and the technical community and the DNS community wanted a better answer than what I told you is the answer, which is you can't. They want behind the scenes for the DNS to be able to validate and to give assurance that when a DNS query is made for www.bank.whatever, that the answer that's received by the resolver that the user is using is the correct answer. And so we developed DNSSEC, the domain name system security extensions. Security extensions is the SEC part of DNS. Next slide, please.

DNSSEC does two things. It answers the question, did this DNS response, what is the IP address of www.bank.whatever, did it really come from the bank.whatever zone? And what they mean by that is, is this really from the domain owner? Is this the data that the domain owner actually signed cryptographically, put in a digital signature that says, yes, this is the correct answer, validate that the keys that are exchanged during this highly technical exchange that happens behind the scenes are the correct keys?

And in doing that validation, it answers a second question which is almost more important than the first question. Was there somebody in the middle? Was there what is called a man in the middle, was there a computer in the middle that was rewriting DNS data that properly came from the zone owner from bank.whatever and rewrite it in transit between the authoritative server from the bank and the recursive resolver that the user has access to?

DNSSEC does this in a very technical way. It uses complex cryptography, it uses digital signatures that are created by domain owners and are uploaded into zone files, and then importantly are validated by recursive resolvers, the resolvers in the middle that take our questions, what is the IP address for this domain name or this website, or this e-mail server, and goes and finds the answer to the question. When the resolver validates the response, it gives the assurance that it's the real response. And it is all of this behind the scenes in milliseconds. So we can say that DNSSEC offers protection against the spoofing of DNS data both at the origin and in transit. Next slide, please.

We also have to talk about what DNSSEC doesn't do. DNSSEC is not a panacea for everything that happens in the world of DNS. It doesn't solve a lot of DNS abuse. Very importantly, it doesn't provide confidentiality, privacy. We assume that everything in the DNS starts from the premise of public zone data, the queries that we make. These are all public data. They are sent to machines that you and I don't control. We don't know who has access to them. We don't know that the data, like our query data, is being stored and then sold or published and used by researchers or used in another way to third parties. We have no control of that, we have no visibility into that.

The confidentiality, the privacy portion of DNS is something that we're going to talk about in our next module, our next workshop when we talk about things like DoH and DoT. But DNSSEC doesn't provide these. It also doesn't address a lot of the really bad abuse that can be used to leverage attacks against DNS software. DNSSEC is not DNS security, it's DNS security extensions, which really are only used to validate the data that's being translated. It doesn't protect against denial of service attacks. It doesn't protect against packets of death. Any attack vector that we talk about all the time in our DNS abuse discussions at ICANN, DNSSEC really doesn't protect against that. Next slide, please.

So, but DNSSEC is good. It's very good. It's also very important. It's very important because it does help to protect, it just does it in a very subtle way. It does it in the way that answers my first question, which is how do we know that when I'm entering my username and password, I'm giving it to the right people. And that’s protecting me and it’s decreasing vulnerability.

DNSSEC is also good because it fosters innovation. After the introduction, the original implementation of DNSSEC, we've been able to leverage it, to invent other technologies that are good, things like DANE, other things that we have that we’re creating that rely on DNSSEC to be in place that can help take DNS to the next step.

So that’s a very basic introduction to DNSSEC that tells you what it does—remember, assurance that the data really is the data that was intended by the domain owner and nobody’s in the middle, nobody is fudging the DNS data in transit. That’s what DNSSEC does at an introductory level. Next slide, please.

So, we want to talk about implementation, because the truth is implementation is a bit of a challenge. ICANN wants everybody implementing DNSSEC. It’s part of our formal recommendations that we make on protecting networks, protecting the DNS and the DNS ecosystem. Any organization you work with that has a resolver, whether it’s an authoritative resolver because it has the domain info for top-level domains, second-level domains, or whether it’s a recursive resolver where you're working with an organization that provides connectivity to its employees, to its members, to its customers, if they're operating a DNS recursive resolver which takes the queries from the users and finds the answers so that the DNS works, so the connectivity is useful, we want DNSSEC implemented. But we have to be honest and we have to know that DNSSEC implementation is challenging. There's a lot to it. Next slide, please.

So, at ICANN, the staff here, we have many decades of experience implementing DNSSEC on resolvers, and that experience has taught us a lot of things.

The first is the learning curve. The initial learning curve isn't that steep. I can teach DNSSEC to any DNS operator in a few hours, or in a day or two, and teach it well so that they come away feeling, “Okay, I've got this, I can do this.”

The difficulty is in maintenance, in documentation. It’s taking everything you learned and everything you know about how to set up a DNSSEC validating recursive resolver or how to properly register DNSSEC information in your zone files as an authoritative resolver operator or as a [domainer.] The challenge is in writing it down, creating good operating procedures and processes and writing it down so that when you're not available, when you’ve moved on, when other people are working with it who haven't received the same training you did, they know what to do. Because continuity of operations over many months and many years has taught us that we need more than one staff member understanding DNSSEC. We need more than one staff member understanding the specific implementation on that resolver in those zone files. So you have to write everything down.

There's tooling that they wind up using, there are scripts they sometimes wind up writing, there's automation that gets put in. And all of these moving parts, these different gears that are going at once, if it’s not well written down, it’s not well captured, it becomes a big issue later on. So we've learned it’s very important to write it all down and to write it all down well.

Finally, there's something called key management, and I'm talking about cryptography keys, private keys and public keys. You all know bitcoin and you know that the key to bitcoin is you have to remember the keys. You can't lose your keys. I think we've all read stories about people who have lost the keys to their bitcoin wallets and have lost millions or many tens of millions or hundreds of millions of US dollars’ worth of bitcoin.

That’s because they didn't manage their keys properly. And they're really regretting it. And the same thing is true in DNSSEC. DNSSEC relies on public key cryptography and digital signatures, and we have to properly manage those signatures. And we have to do so with the assumption that I'm not going to be here tomorrow. I'm the key manager, I'm setting up DNSSEC. I have to build it assuming that I'm not going to be at the organization tomorrow, for whatever reason, good or bad. Somebody else needs to be able to pick up this key management and the keys have to be properly protected.

So, this is just some of the high-level lessons that decades of experience have taught us. But there's some good news. Next slide, please. My colleauges and I have developed courses to do this, to build hands-on skills with DNS and specifically with DNSSEC. And these courses are available.

When you think about your constituents, the nonprofits you work with, if you can, if there's an interest in setting up DNSSEC on either the authoritative and/or the recursive side, we can get together with you. If you work with your local Global Stakeholder Engagement representative, we can work with you to put together workshops, hands-on workshops that can take day, half a day, ideally they take two days. Two days is the perfect DNSSEC workshop. We can get together and we can teach you this with laptops, with everybody working at a computer actually learning how to set it up through these wonderful modules we've created and we work with you on.

We also do this at ICANN meetings. We just finished ICANN 70 and we had a nice DNSSEC workshop. It wasn’t so much hands on, but in face-to-face ICANN meetings, we do all day workshops typically where we can teach all about DNSSEC. These resources are available to you when you work with your GSE representative, your ICANN Org friends. We can help. We can offer these. And what's nice about this is we all make contacts. Your constituents get to meet really good and skilled engineers who understand DNSSEC who are also good teachers, and they get their contact information, they shake hands and they exchange business cards, and they've got a resource. And that resource becomes invaluable over years and decades, as you all know.

So that is our basic overview of DNSSEC, what it is and why it’s good. That is an overview of some of the resources that are available to you as the NPOC for how we can get hands-on skills and build skills in DNSSEC, and importantly, do the community building and the networking that’s necessary for DNS operators who are doing things like DNSSEC, because they always want to have access to other people to ask questions.

That is the end of my slides, and welcome any questions, because I think we’re in a Q&A portion. So otherwise, I'm going to turn it over to Adam.

ADAM PEAKE: Thank you very much. Thank you, David. Thank you, Brian. So I think now we can open it up to all of you if you have any questions. And Caleb, if there's anything that you would like to lead on here, that would be great. But I don’t mean the questions, but if you’d like to help manage this portion of the session. I thought it was very good and I saw some connections between what Brian was saying about how you administer some of the more basic aspects of domain names, making sure that you know what the e-mail has been used to register a domain name, that you know that the contact information is up to date, because I know from my own experience before joining ICANN that working for a smaller NGO and some of the larger NGOs, technical operations are difficult and you might ask a friend or a volunteer to help you set up the DNS, and of course—or it could be somebody that just leaves the organization, and you can end up not knowing what the contact information is for this incredibly important resource. And as we've mentioned before, a domain name is when you're setting up the technical system for your nonprofit, the domain name is not the most expensive part of this by a long way. They're quite a low-cost item, but they're incredibly high value. And I think we can connect this to what David was saying about DNSSEC key management and the work you will do there. You need to make sure that this information is documented so that people understand what systems are in place, what versions of software are in place so that you know when something needs to be updated and so on.

So there's a very important thread here, I think, of running through the internal administration and management of the domain name system. On its face, it can sometimes look quite simple, and I think it’s actually much more difficult, and we do hear of problems and we've always heard of problems, particularly for smaller organizations, where volunteers, friends, contractors, people who leave and move on might have the essential information that you need within your organization.

So with those thoughts, if we’d like to pass it on, any questions? I just want to say that, yes, for those of you who’ve been asking about the archives, all of this series are available online. They are being archived, you will be able to find the full Zoom record, audio transcript, written transcripts, a chat record and so on, and Brenda and I have both put this into the chat a couple of times, and perhaps Caleb, when we do a review of this, it could be sent around to the NPOC list so that everybody is aware that these archives are available, because they are of course here for you.

Okay, thank you. Any questions and comments? Thanks.

CALEB OGUNDELE: Yeah, Adam, it seems we have one question from Ken in the chat room. Maybe you might want to touch on that.

ADAM PEAKE: Right, so I think David or Brian, the question is a lot of organizations will be getting their DNS services from their local ISPs. How can they learn whether or not the DNS provider has implemented DNSSEC, and what should they do if they find out they haven't? I think is the follow-up question to that. And what do they do if the provider is implementing DNSSEC? Is there anything for them to watch or manage in that case? So, thank you, over to one of you two.

DAVID HUBERMAN: That's a great question, Ken. Thank you for asking it. In our workshops, we teach how to investigate whether a resolver has DNSSEC turned on. There are tools we have available to everybody freely you can use at your computer right now or home office right now that can test, that can probe very benignly whether an ISP is using a resolver that has DNSSEC validated or not. It's a fairly simple command line process.

If they're not, that's a really interesting question. That is a question of finding the staff at a local ISP who are responsible for DNS and asking them to turn on validation. That is a [challenging proposition] on how we can best motivate and persuade ISPs to turn on DNSSEC validation. That will often require the personal touch, knowing and being able to get at the people who make those types of decisions.

CALEB OGUNDELE: Thank you, David. So, can I ask a question as a moderator here? I think I can. So this is just perhaps for members to get some ideas. So I noticed that most times, NGOs do not develop their websites themselves, they do not register the domain names themselves. They tend to contract it out to a web developer [who gets to do stuff for them,] and at some point in time, they find it very difficult or perhaps [inaudible] move away from the web developer to someone else. They usually find it very difficult because that person might not be releasing access to the domain names to them.

What do I mean by that? Helping them change to the next nameserver that they're going to be using. So in the case of domain name disputes when this arises, how is that going to be sorted out as a registrant?

ADAM PEAKE: I think that’s a good question. I wonder if Brian, you might have an answer, or David. We've heard this before, that a web developer may have registered the actual name for the organization so they're the person in the record, and of course, they're registering it for you, but is there anything you can do, or have you come across this type of case, Brian? It may be something that you’d be aware of. And if not, then it would be something that we’d ...

BRIAN GUTTERMAN: Yeah. Thank you. I don't know if David, do you want to take that?

DAVID HUBERMAN: Sure. It’s a great question, Caleb, and it’s probably a very common scenario. This is where it’s really important that we have good education with our constituents. When you're setting up a nonprofit site or when you're thinking about the site that you already have, it’s really important to think about who owns the domain, where is it being registered, who is registering it and who controls those credentials. Brian gave very good information on how to secure those credentials and interact with those credentials in a secure way.

But there's a more basic question that Caleb asked, which is, who owns the domain name? And it shouldn’t be the web developer, it shouldn’t be the third party. It’s really important that nonprofits, when they're thinking about their online presence, retain control of these things, these assets. They have to do the domain name registration themselves, or they have to contractually maintain control over the process with a third party doing that type of registration.

It’s okay to have a third party do your registration for you, as long as contractually, the credentials and the ownership falls to the nonprofit. And by the nonprofit, it depends on your legal jurisdiction of course, I'm not giving legal advice here, but let’s think about this very carefully. It’s the nonprofit that wants to own the domain name, not the person, not David and Caleb, we've got this great nonprofit to help people. It’s kind of important that it’s not Caleb who owns the domain name and it’s not David who owns the domain name. It’s actually the nonprofit. Because we’re not always going to be around, while we hope our nonprofit lives forever.

So think real carefully when you're thinking about online presence, when you're helping your constituents in these issues. Think real carefully about who should own the domain name and contractually within your jurisdictions, how you set it up so that the third parties you work with don’t get control that the nonprofit should have.

I don’t want to evade the specific question you asked, Caleb, but I can't give you a great answer, which is when this is already happening and there's already a dispute, it’s going to be a fact dependent, case dependent resolution, and you'll have to avail yourselves of local law and legal jurisdiction to figure out how to resolve it. So that’s my response.

BRIAN GUTTERMAN: Thanks, David. That was very comprehensive. And again, a great question, and it goes back to some things we emphasized on our earlier webinars. Again, if you weren’t able to join the previous webinars, we encourage you to access the recordings, have a look at those. Also when you're thinking about talking to nonprofits who might not be here but who are interested in NPOC’s work and engagement, to go back there, remember to treat these domain names like assets—again, these are some of the things we want you to take away. They're assets.

When registering them, remember whose credentials were used, and if somebody is leaving the organization and they were involved, like you said, in the operations of the online presence of the organization, make sure that their information is passed along in a secure manner to somebody who will be taking over those duties, whatever it may be. And these things can help.

And yes, I see another question about DoH and DoT and DNS privacy. This is a perfect opportunity to preview next week’s webinar where we will be covering that. So, thanks for that question, and a plug for everyone to join next week. That’s it for me. I pass it back to Caleb or Adam. We can wrap up shortly if there's not any more questions. Caleb, is there anything you wanted to say to the group or any reminders, any PSAs for NPOC members here?

CALEB OGUNDELE: Thank you all for making the time to attend this webinar. The NPOC leadership is really excited to have very high number of participation in this webinar, and we really look forward to having you participate actively next week.

We are taking note of all the questions and suggestions that we are seeing in the chat room where some folks have requested additional topics that they would like the ICANN team to cover, and we will put that into consideration and have a conversation with them.

So on that note, thank you so much to Adam, David and Patrick, Brenda, Maryam and all ICANN staff that are in attendance, and Brian as well. So thank you so much for taking the time to share some of this knowledge with us, and we do hope that we'll put it all to use. Thank you so much, and over to you, Brenda, to close the meeting. Thank you all for coming.

BRENDA BREWER: Thank you, Caleb. Adam, do you have any final words?

ADAM PEAKE: Only to say thank you, thank you particularly to Brian and David, and look forward to seeing you all next week. Thank you so much. Cheers. Bye.

BRIAN GUTTERMAN: Bye everyone. Thank you. Have a great day.

**[END OF TRANSCRIPT]**