JOHANNESBURG – At-Large AFRALO ALS Capacity Building Session 2
Tuesday, June 27, 2017 – 08:00 to 09:00 JNB
ICANN59 | Johannesburg, South Africa

UNIDENTIFIED MALE: This is the ICANN 59 At-Large AFRALO ALS Capacity Building Session 2, 27th of June, 2017, 8:00 to 9:00 in Ballroom 4.

AZIZ HILALI: Hello, everyone, and welcome to the second session, Capacity Building session that we organize every day at 8:00 in the morning. Our topic today will be challenges, security challenges having an impact on registrants and end users. It's a very important topic. This is why we wanted for this second session to talk about it and I have the pleasure today to introduce to you our two speakers and I would like to thank them very much for coming this morning to talk to us.

Steve Sheng on my left is the Director for the SSAC and RSSAC Advisory Development Support, and we have Mr. David Piscitello, who's VP of Security and ICT Coordinator. I would like to thank them very much and give the floor to Steve Sheng. Steve, you've got the floor.

STEVE SHENG: Thank you, Mr. Chair and Vice-Chair. It's a pleasure to be here today. My name is Steve. This is my third time in Africa, and every time I come here, I just felt very welcomed and feels like coming home, even on the South African flight, just felt that. So, it's very good to be here.

As I said, my name is Steve. I work in the Policy Department. Our team supports the development of advisories for the Security and Stability Committee and also the Root Server System Advisory Committee.

To my left, I'd like Dave to introduce himself, a former colleague of mine. And now Dave.

DAVID PISCITELLO: Good morning. I'm Dave Piscitello. I'm the Vice President of Security and ICT Coordination at ICANN. I work in the opposite Chief Technology Officer and I'm part of the Security, Stability, and Resiliency Team.

STEVE SHENG: Thank you. So, we want to make the section today a bit more interactive and also we want to focus more on the registrant and also just touch a bit on end user. But I want to begin by setting a context and a framework. When we think about security threats or security issues, these are largely can be divided into three

categories. The first category will be called a physical attack. These are the kinds of attacks that actually attacks the infrastructure, attacks the telecom infrastructure, ceiling, cutting the cables. So, you have the physical attack.

The second part of attack is what we called syntactic attack. This is attacking how the workings, how the protocols that runs these systems is attacking the vulnerabilities of those protocols themselves. You've seen attacks, for example, the latest one, the ransomware, where is it using a Windows exploit, and use that to insert ransomware on people's computers, and use that as a means to extract money.

Another example of the syntactic attack is the denial-of-service attacks, where a malicious attacker pretends to be trying to flood the legitimate traffic and an example of the DNS, you get a response before the [inaudible] send the response back, so you, as an attacker, now you're in control.

So, those are the ways a syntactic attack is attacking the protocols, the design of the protocols, the vulnerability of the system. So, we have the physical attack, the syntactic attack.

And the third category of attack is what we call the semantic attack. This type of attack is attacking how humans assign meanings to the interface they're interacting. A prevalent example of that attack is phishing or spearphishing, where in

this context, the person or the malicious attacker setting up websites and present that to you as if it is from the legitimate source.

So, from the user perspective, you assign meaning based on the content you see many times, and therefore, it's gaining the trust of the user and then you give your information away. So, these three types of attack, we see different varieties and within different continents, the prevalence may be – the emphasis may be different.

For example, in Asia, the social engineering attack is not about setting up webpages, but mostly calling you on mobile phones or stopping you in the street corners. That level of attacks is different from continent to continent.

With deep apologies, I don't know very much which these types is prevalent in Africa, but I want to set the context for you to think about the problem in this space as we go into security trends impacting registrants.

Next slide, please. Next slide. Next.

So, when we talk about kind of threats to registrants, these registrants, the ones that register domain names or you have one domain name in your portfolio or you may have many

domain names. Again, there are two types of threats. You have the external threat and there's the internal threat.

From the external perspective, here you presume an active attacker. What an attacker will usually do is he or she, or an organization, will seek to gain access to your registration account and to control the angle of that is to control your domain name. Right? So, you usually have a relationship with the registrar that sells the name to you or with a reseller that you go through to get your domains. And they usually attack the registration account. The goal is to control your domain name.

The other part, somewhat related, is they're trying to gain access to your registration account and their goal is to change the DNS information associated with your domain name. What do I mean by that? You register a domain name, you probably will have a web presence, you have a website, you may run your mail server, and you have these records in the registration account.

When an attacker gained access to it, he or she will insert a set of new records, change the IP address, where the website should be going to, where the mails should be going to, and he does this in a variety of ways. He may want to use your account and use your system as a part of a larger attack network. Or he may just

want to use this to deface your webpage and try to get some money out of it. So, those are what I call the external threats.

In terms of internal threats, and this is really the domain names have reputation and residual value. When you register domain names, the domain names will register the renewal rates are fairly high. That's because they have the residual and reputation value, and there's also, in some cases, a quite high switching cost to change to a different domain name.

Because your domain name has value, there will be people closely monitoring your name. If sometimes you fail, you just forgot to renew your name and after the grace period, I think, which is five days, someone else will register your name. In that case, in that scenario, the name becomes his or hers. Subject you are exposed to a very high cost and lengthy process to claim your name back. So, I want to, again, set the context thinking about this type of threat. I'm going to go over those in a bit detail.

So, next slide.

When we talk about unauthorized access to the registration account, how do they do that? How you as a registrant or how the attacker do that? You know, you want to be able to understand how the attacker does it in order to protect yourself.

The most obvious one is the guess attack. An attacker would guess your account name and password at your registrar. You may wonder, this may be unlikely farfetched.

Before I joined ICANN, I was doing the PhD research looking at usability of security systems, and one of the things our lab does is to look at passwords, how secure passwords are. We find interesting things. One, people reuse passwords through multiple different accounts. You have it for a bank and you have it for your registrant account, and you have, and you reuse in many other places, so that means when an attacker gets hold of one set of your credentials, he or she will try to use that to the other set of logins you have, so that's one weakness.

The second weakness is that what we call the entropy of the password, meaning the guessability, how difficult to guess. It's actually very, very easy to guess. So, my advisor produced a poster of the thousand, probably not tens of thousands passwords and they did this analysis and the common ones, I love you, these are usually the tops ones, and you have lots of easy passwords, very easy to guess. An attacker, one way for an attacker is to guess your password. Dave.

DAVID PISCITELLO: How many of you have a password that's longer than seven characters? Good. 10? Pretty good. 15? Okay. So, at ICANN, we're

required to have passwords of 20 characters or longer, which can be very, very challenging. How many of you use some sort of password manager on your computer where you store your passwords in encryption? One of the things you really ought to consider. Okay, you're the pro here. So you really ought to consider using a password manager. Many of these generate strong passwords for you and they keep them securely stored on your computer with encryption, and several of them actually have software for Android or for iPhone or iPads so that you can use it on all your devices, so this is a very, very useful thing to do.

I also want to point out that guessing passwords is actually not the easiest route for attackers. The easiest route for attackers these days is to compromise a password database at a website that you visit and then make assumptions, as Steve said, that if you've created this password, you may have used it elsewhere, and so if what they can do is go to thousands of sites using scripting software and your e-mail address and they'll try your e-mail address and a password at thousands of sites, hoping that they actually hit a site that you have visited, so that they can now get into that information.

This is why it's critical that you do not use the same password for your banking or as you do for anything else. And even more importantly, if you bank at multiple banks, always use a different a password for each of those banks.

STEVE SHENG: Thanks, Dave. Just quickly moving on, there are other ways the attacker can capture from the host containing credentials. This may be your computer or the server. Sometimes we store these credentials in clear text. Sometimes my wife maintains this Word file, listing all the password, all the login account that we have. It's true, I mean, even for security professionals, and then we move on to, as Dave mentioned, to password managers.

Another way, talking about social engineering, we talk about phishing attacks and spearphishing. And phishing and spearphishing is usually the first step to compromise to get into your computer. What they usually want is to install a piece of software, you call malware, that can capture what you type and can intercept, sometimes intercept what you send.

The typical scenario is this. You receive an e-mail from your registrar saying, "Alert, alert! There is unauthorized activity to your account." Sounds. You may think, "Oh, okay." There's "Please log in here to confirm that nothing has changed." So, that's quite common from the registrar and registry perspective sometimes. Obviously, those was not sent from a registrar. And when you enter those in, your account will be compromised or sometimes they ask you to download something to help you secure. In that case, your computer will be installed a malware

where additional information, not just your registration account, are at risk.

Next slide.

The unauthorized access is the first step. It's a means to an end. It's not an end itself. So, what's an end here? The end, one, is to change your DNS configuration information.

It does it a couple ways. They change your name server to something else, other than the address you intended. This, of course, what [would] happen is it will result in a loss or disruption of your servers, whether it's your website or your e-mail, and it's the traffic is being redirected to the attack server. Sometimes lack of coordination or administrative error can also introduce changes with similar consequences.

Next slide.

Another aspect where unauthorized access is a precursor to… is they want the attacker wants to change the contact information on your account. Why do they want to do that? They want to do that to take control of your domain name. In this case, transfer or wrongfully taking control of the domain name. That's what we call domain hijacking. Obviously, another thing they do is they want to disrupt the server's delivery of registrar correspondents. So, usually the first thing that the attacker do,

they go in, log into system, they change your e-mail address where registrars contact you.

So, if you're relying that communication channel with registrars to receive important information, now you don't receive them. But many cases, many of us are receiving too many e-mails a day, so if you're not receiving that from registrar, you forget about it until sometimes it's too late. It's my point.

And because when they fill in wrong information, this could also lead into filing a report of WHOIS inaccuracy against you, which could lead to a suspension or the deletion of domain name by the registrar. With the new RA in place, there's certain level of accuracy verifying checking, and failing in WHOIS accuracy could lead to suspension.

And finally, it would just lead to the deletion of the domain name registration by the unauthorized party. So, that's kind of a very high-level overview of the threat as a registrant you may be facing and how attackers does it. So, before we go anywhere further, I'd like to open this up to questions.

GABRIEL BOMBAMBO BOSEKO: Yes. I would like to know if ICANN – my name is Gabriel. I'm from Congo, I'm from Kinshasa and I would like to know does ICANN take steps to work with governments that are

responsible for external threats and attacks against end users? We have many opposing political members and we have seen the use of those attacks coming from the government against the websites of the political opposition. Does ICANN do something about that?

STEVE SHENG: So, let me see if I understand your question correctly. You're speaking about a situation where a government attacks a user in his own country or a government attacks a user in some other country. So, there are two different things. One is oppression and the other is terrorism.

We do not have a role in that kind of interaction. Our role, even in the security realm, is primarily one of facilitation and subject matter expertise.

So, if we work with a government, it's usually something that relates to the government's sovereign oversight of their country code top-level domain. So, for example, ICANN has relationships with 261 country code top-level domains so that their information is in the Domain Name System and people can go to domain names or websites or receive mail from citizens and users in any country, and they'll all be directed correctly through the name resolution process.

And so that's our primary role through what we call the IANA, which is now I think the PTI, which is the Post-Transition Internet Assigned Names Authority. Right? From my team's operational level, we will work usually in threats to the global Domain Name System. So, we may work in cooperation with governments if a government website were being attacked through a denial-of-service attack.

You may remember years ago that the government of Georgia website was attacked and so we worked with other operational security people to try to quash that attack. But we don't get involved in any sort of confrontation or conflict between any parties, government/government, user/user, government/user.

UNIDENTIFIED MALE: I have two questions, remark, and a question. There is a what we call the [inaudible]. When you write a domain name, you have a mistake if you have typosquatting to give the impression to the user that you are in a particular set and you're not. The typosquatting so it looks like a webpage from a bank and it's not.

My second question will be after Gabriel said. Gabriel talked about governments and citizens and we would like to know is whether the dangers and the threats that we do have with

elections, especially when we have several states like it might have happened in the United States.

DAVID PISCITELLO: Answer the first question. I think you're talking about cybersquatting. So, there are some guidelines and some rules about cybersquatting in the ICANN policy that and you can petition to have that name removed from the Domain Name System. There are some threats that actually evolve from typo squatting in what is called name resolution rewriting, and this is actually something that is used by commercial entities. And what happens is a hotel or a coffee shop, anyone who's offering wireless, will partner with someone who wants to monetize your typing errors, and so if you type wwww.ebay.com, this service that the hotel or the kiosk subscribes to will take the answer from the Internet that says there's no such name and it will redirect you to a search page that is being promoted by a company, I think, one of the company is called [Bear Fruits].

And then that page has advertising and it's not really where you wanted to go. What you really wanted to know was oh, I've mistyped and I didn't get to eBay as I expected. So, this is actually a threat and the Security and Stability Advisory Committee wrote a report on this a few years ago and I've written a blog to follow up on that. It's really, really bad because

what it does is it tells you a lie. It tells you that there is a place to go that has this name where there really shouldn't, and the answer should be no.

So, that's something to be aware of and you are working someplace remotely, one of the things I would suggest to you is that you configure your laptop or your phone to always use a name server that you trust, whether that's OpenDNS or Google or some other very, very large name service. Google is very easy to remember. It's 8.8.8.8, so I tell people that if you know how to open up your configuration and you can go and just set that statically, then no matter where you go, you'll always be getting the same name resolution and you won't be getting any of these lies. So, that's what I would suggest for cybersquatting.

STEVE SHENG: Let me try to answer the second question, where these kind of phishing or security attacks that compromise end user credentials that leads to stolen e-mails that happens at the very highest level. I think it's safe to say it is outside ICANN's remit because ICANN's remit is coordination of the allocation and assignment of identifiers.

Nevertheless, I think even our organization employees in our organization have to go through these trainings so that we, as employees, don't fall for spearphishing attacks and I have done

research in this area personally before, so I can point, provide some pointers to you afterwards, but that's really not ICANN. It doesn't fall ICANN's mission or remit to educate users about these types of attacks.

DAVID PISCITELLO: We actually don't have that in our remit but one of the things that my team does is publish periodic articles on security terminology and security threats, so for example, today I'm publishing an article on the Dark Web in the ICANN newsletter. We've published articles man in the middle attacks and covert channels and other things, so if you go to the ICANN blog and you search on the security term, you'll often find something that we've written that's informative at a level of Internet user. It's mildly technical but the idea is to help people understand different threats.

AZIZ HILALI: Thank you very much. We still have four persons asking for the floor, so please try to be fast. Tijani first then [inaudible]. Tijani, you have the floor.

TIJANI BEN JEMAA: I think that now Steve said it but when you answered the question of Gabriel, I think you didn't say that it was out of the

remit of ICANN because ICANN is in charge of the unique identifier. The security of the root servers is the duty of ICANN but anything between the user and government and the registrar is the contract is between user and registrar. So, ICANN cannot intervene in it and doesn't have anything to do in it. Thank you.

DAVID PISCITELLO: I just want to correct you about the security of the root servers. ICANN actually does not have the responsibility of the security of the root servers. We only have the responsibility of the integrity of the root zone, so each of the root server operators is responsible for their own operation. So ICANN does have the responsibility for L-Root and we take that very seriously, and I think that we do a fantastic job. But ISC and the Department of Defense in the United States and RIPE and others are responsible for the operation of their own root servers.

AZIZ HILALI: Thank you, David. [inaudible], you have the floor.

UNIDENTIFIED MALE: Thank you. [inaudible], Consumer Federation from [inaudible]. As representative of consumers, I'd like to ask if ICANN has some statistic data to know what kind of danger for each region. For

example, if today I have to organize a campaign on security, we can say, "Okay, Africa, there is no dangers but do we have some statistic data to know what are the danger for each region, so we can say that you're not in a very rich region but you have to take care of this kind of danger for this region." Thank you.

STEVE SHENG: If I understand correctly is from ICANN perspective, if we have data threats data for each region. I'm not sure we do because I don't know in some cases how we get that data. Right? We have a narrow remit and the data to the extent possible, some of these data are mostly security companies would have them. Maybe some registrars would have them but it's not clear to me, so I'll have to think about that but I do recognize that's a valid question. Let me think about that and get back to you.

DAVID PISCITELLO: ICANN probably doesn't have threat data at the regional level. However, if you go to the Anti-Phishing Working Group, I know that they have a report on mobility and mobility threats and that report is probably two years old now, but at the time, one of the significant threats for the Africa region was mobile operating system, a large number of service providers in Africa do not provide automatic updates to Android software, for example, and many of the devices that are sold in Africa because of the

need to keep the price down aren't upgradeable after a certain number of operating system upgrades. And so this becomes a problem because a vulnerability remains in the entire population of that carrier for a very, very long time. So one of the things that each country could look into in order to reduce the threat to its users is to go and create standards or obligations for the carriers to maintain what we call patch currency on operating systems, and that's a challenge because it's an economic issue.

If you want to bring a device to millions of people at a very, very low cost, often what you do is compromise on the amount of memory that you put in a device, and then operating systems get bigger as they add features, and so you can't get everything into this small device. So, now you, the carrier sits there and says, "Well, how do I serve the population with an inexpensive device and keep the devices secure?" So, that's a challenge that I think this region has because a number of countries are emerging technology nations.

I'm trying to think. I know that Symantec has regional statistics at their site and McAfee has some regional statistics about threats at their site. Currently, there are a lot of companies that are trying to promote security against ransomware. Is everyone familiar with a ransomware attack? Who doesn't know what a ransomware attack is?

Okay, so a ransomware attack is usually an e-mail attack and when you go and you receive a document or some attachment to an e-mail, when you click on that, software is installed on your computer, and then that software contacts another computer and downloads encrypting software, and it encrypts all the data on your computer and then it locks your screen or it locks your computer and says, sometimes it imitates police or it imitates some sort of tax agency and says, "Your computer has been seized. You must pay a fine to this address or to this entity or we'll erase your data forever." And so what the attacker is doing is he's holding you for ransom and if you pay the fine, you are supposed to get the key that decrypts your data.

If you're interested in learning more about that, because we don't have time, I've written some articles about that at ICANN and I've also got a presentation that I'll share with the ALAC staff and distribute to you. So, that's another very, very big attack that's actually global but they've been doing a really good job of localizing it into local languages. Even the screens that come up are in Arabic or in French, very local language or they're very, very sophisticated.

AZIZ HILALI: Thank you very much. We still have a lot of questions and we have questions on the chat, so we are going to try to get quicker.

[SERGE]: Hello, everybody. I'm [Serge] from Congo, Brazzaville. I have two questions that I'm going to ask. First question about the impact of IPv6 for the implementation of IPv6 has an effect on DNS. Is it related to a failure? And if there is a failure, how can we resolve this problem, and my second question is what is the possibility to implement a system to observe the security issues in the countries? ICANN is about to help us in this way. Thank you.

STEVE SHENG: So, for your question about setting up, essentially, monitoring centers, I think that it's fair to say it's far from ICANN's remit. Some of the relevant resource that could be available to you is what we call the CERT, the Computer Emergency Response Teams that have the CERT in many countries and in U.S., you have the CERT Coordination Center. So, if you're thinking about that route, I will encourage you to contact them and gain some assistance there.

DAVID PISCITELLO: So, bear in mind that ICANN doesn't govern the Internet. It's like ICANN is only administrator and really a delegator of the responsibility of identifiers. So, one of the things that we do is hand responsibility of domain names to top-level domain

registries and they become responsible for what we delegate to them. So, Verisign is responsible for .com. We can't actually go in and tell Verisign, "Do this," unless they're in violation of our contract with them. We can't go and tell them, "Remove a domain name." Law enforcement or an individual would have to do that directly to Verisign.

That's sort of setting the context for my next answer, is the kinds of threats that we monitor at ICANN through our central operations are failures in the name system at the top level and root. So, we have a program in ICANN in our operations where we check to see that what's called the authoritative name servers for all the TLDs are operating and responsive, and when we see that they're not, we contact them, so at the very high level of the DNS, we have an operational process that tries to ensure the availability and the resiliency against failure of the name server space, and that's probably the most operationally involved we get.

We also test to make certain that all the zone files in the top level that support DNSSEC are assigned and the signatures are working correctly, and so we monitor the cryptographic integrity of the top level, as well.

AZIZ HILALI: Thank you, David. I'd like to give the floor to all the one who wants to have to ask a question, so please just one minute for the question and two minutes for the answer. So, I have Bakary, Ali, [inaudible], and then we'll see if we have time for the questions in the chat. Bakary, you have the floor.

BAKARY: Thank you very much. Bakary, Internet Society from Mali. I have a question about final users. We know that among those attacks, some entities are the aim but the user pay the most price, so among those attacks, are there some attacks aimed to the entities or to the final consumers? First question.

Second question about the security of domain name. It is not the user, final user, who is responsible. If I fear that my domain has been attacked, can I ask the registry to solve my problem?

AZIZ HILALI: Okay, we are going to take three question and then you will answer. Ali, you have the floor.

ALI ALMESHAL: Questions. Just a clarification from Steve when he was making his presentation, the domain renewals, do you have five days or do you have 30 days? Because and who sets this? Is it just

registrars or registry? There seems to be some deviation because, usually, from what I know, it's about 30 days, but now I hear it's five days, so where's the deviation? So, that's one.

My next question is to, sorry, I didn't get his name, the gentleman sitting next to Steve in the yellow shirt. That's you. David. David, you talked about password managers. I have dutifully avoided using password managers simply because I have a suspicion that you're putting all your eggs in one basket. If somebody hacks into your computer, you have basically left all your passwords on a silver platter. Please disabuse me of that assumption or confirm it. Thanks.

UNIDENTIFIED MALE: Okay, just one question. I have two questions. I'm [inaudible] from Republic of Congo. I have two question. First, I'd like to know if ICANN has a resolution or sanctions for attacks from a country to another country? And the second question, do you have a system in ICANN to study the new applications that are online so you can tell the user that there are some failures for the user and to fight again the attacks? Thank you.

STEVE SHENG: So, my deep apologies. I have to go very soon to support another session. But on the domain renewal grace period, I think there

are multiple grace period. The one you know maybe those added together would amount to 30 days. I have to confess I'm not an expert in this area, but I will – and Dave can corroborate – but we'll get the correct information to you.

Regarding the question WHOIS why the user is responsible, I think in some sense, we all share responsibility, right? I mean, from a broader perspective, you want to assign responsibility to the person who can actually fix the problem. I think users play an important role for that. We just cannot rely everything on registrants and registries for our poor behaviors. We have a part in that. Obviously, registrars and registries have responsibility themselves, right? So, I think a fight against us, everyone plays a role, but we should place the responsibility on the entity and the persons that can fix the problem.

So, those are my quick two answers. My apologies. I have to leave, but I think my colleagues from ALAC have my credentials, e-mail addresses, so Yesim or Ariel, feel free to please to the delegates and I'm happy to answer those questions in e-mail. Thank you.

DAVID PISCITELLO: Thank you, Steve. I'll be able to stay for a bit longer, so I'm happy to try to answer as many of these as I can remember. I'm getting old and senile and it's a challenge. I wanted the

comment about or follow up with what Steve was talking about in terms of responsibility and accountability.

When you register a domain name, it is like leasing an apartment or leasing a home or getting a license to drive. You have a responsibility for now, deciding what you're going to do with that domain name. One thing that you can do with a domain name is run a mail server. You can also host a website.

Who do you choose to actually do that run the mail server for you? You often choose your Internet service provider or sometimes you get that service from a third party. Sometimes you host your blog at Typepad. Sometimes you host a web at a local web operator.

Now you have another party that you've paid to or you rely on to provide your hosting for you, and so you're responsible for the name but he's responsible for the operation of the web. Right? And that's different in many cases from the registrar from whom you got the name and the registry from whom the registrar pulled the name.

So, there are lots of different parts in motion in actually putting or publishing information or sending mail. When someone is attacked, one of the things that I'm involved in because I work operationally in security, is trying to understand where the attack is coming from, what did they attack, who is the

responsible party, who's accountable for correcting or mitigating the threat, and it's not simple. It's a very, very complicated situation that gets complicated even further when it happens across jurisdictions, when the web server is in the Netherlands and the person who's attacking is in Croatia and they're sending bitcoin to somebody who is in Latin America.

And so I find the job that I have is extremely exciting because you really have a very difficult puzzle to put together into ultimately find a criminal and then be able to serve a warrant and put him in jail. Right? And ICANN doesn't serve warrants, obviously, but we work with law enforcement to do things like that. So, I think, I hope that answered your question.

On the five-day, 30-day, which is the number? There are actually multiple hold periods and the first one is called the add grace period. So, from the time you actually complete the registration of a domain name, you have five days, which is called the add grace period, to make certain that that was the name you wanted. Yeah. Sometimes, people mistype, even when they go in they do a registration, and so you have five days where you can go and you can say, "No, this was not the name," and you don't get penalized, you don't lose your money. It's like being able to return a garment to a store. You have the receipt.

And then if you have registered a domain name for a year and a year comes up and you haven't actually renewed it, you have 30 days after that year during which the name is held and no one else can register it, so it's basically called on hold and you have 30 more days after your expiration before the registrar will say, "Okay, this person clearly doesn't want the name. I'm going to hand it back. So, did I answer your question, Ali?

Okay. Password manager. Password managers use strong encryption. I would never recommend that you use a password manager that doesn't encryption information because there's no point in doing that versus notepad. But most password managers today use AES 256-bit encryption or stronger, which is not something that is just leaving it out for anyone to read.

The value of a password manager is that you can remember one password and create one strong password, and in fact, the way many password managers work, I use one password. You can have it generate all the passwords for you and you never have to remember them, and it will automatically fill in when you visit a site with a password that you have generated. So, what I often do is, and with my password manager is I say, "Make a 24-character password." I don't know what it is and so but every time I go to that website, it'll fill it in for me, so I don't have to remember. And I find that very, very useful.

Country-to-country attacks. ICANN is not a government body. We don't participate in the United Nations. We don't participate in Council of Europe except as an observer. We don't participate in any sort of government-to-government interaction. Our only interaction with governments is to encourage open Internet and encourage an open and unified DNS, and support the governments in their technical name service operations.

So, we're not a policy organization that respects. We don't have any policies about government/government sanctions. And then what was the last one? New apps and features. We're also not a software developer or a testing agency. So, for example, if you want to buy an app from the iTunes Store or from the Android Play or whatever, we have no input to that other than an app that we might develop.

Occasionally, if there's something that looks like it's affecting the DNS and we know or we're aware of a vulnerability in an app, we may write some sort of advisory and put it up on our website, but that is not something that's normally in the scope of our activity.

Did I answer them all? No, that's fine. I'm just trying to answer your… You piled all these questions on me. You can't then tell them I can't answer them.

AZIZ HILALI: Thank you very much. Those questions show that the decision was very interesting, so thank you very much, Dave and Steve, for this presentation.

I'm going to ask the participants to if they are interested, to follow up this discussion online. I think everybody is very interested, so now we have to finish because we need to leave this room because there is another meeting now, and we need to give some time for the interpreters that I want to thank. Tijani, you want to speak?

TIJANI BEN JEMAA: Thank you very much. For the Capacity Building program of ALAC, we have a webinar on this topic with Steve that we made with Steve. We had a lot of following today. I see that a lot of people are interested. So, if you want us to organize a webinar on this topic, just ask for it. We want to some webinars interesting everybody, so you just have to ask for it. Thank you.

AZIZ HILALI: Okay. Tijani's asked me to close this meeting, so thank you very much. Thank you, Dave, Steve. Thank you to the interpreters, to the staff, and see you later.

[END OF TRANSCRIPTION]