HOW A HACKER STOLE KZRA.COM – WITH MAILYNNE AND CHRISTIAN CALVIN

August 28, 2017
Episode 403

DOMAINSHERPA.COM

MICHAEL CYGER: I've heard of domain names being stolen many times in the past, and each time I reach out to the investor to express my support and determine if they figured out how it was stolen. What was the root cause? Because I want to educate others, so they can prevent domain theft from happening. But each time I reach out, I'm disappointed to hear they have no idea how it was stolen...until today. We're going to learn exactly how a domain name was stolen, so stay tuned to hear all the details and learn how to protect your domain names.

Quick message from three of our sponsors that helped make this video, show, and podcast possible.

First, if you're buying or selling a domain name or portfolio and you want an estimate of it's value, Estibot.com is the place to go. Just like you'd visit Zillow.com to get an estimate of a house value, Estibot.com provides key information about the most important statistics so you can make an informed decision based on data.

Second: Serious about online trading? Secure your funds, keep your merchandise safe, and use a company that keeps the buyer and seller protected the whole way through. That's Escrow.com. Payments you can trust.

Finally, if you're a domain name investor, don't you have unique legal needs that require domain name technical know-how and industry experience? That's why you need David Weslow of Wiley Rein. Go search for David Weslow on DomainSherpa, watch his interview and you can see for yourself that he can clearly explain issues, can help you with buy/sell agreements, deal with website content issues and UDRP actions, and even help you write your website terms and conditions. David Weslow is the lawyer to call for Internet legal issues. See for yourself at DavidWeslow.com.

MICHAEL: Hey, Sherpa Network! Thank you so much for joining me today. My name is Michael Cyger, and I'm the publisher of DomainSherpa.com, the

website where you can learn how to become a successful domain name investor or entrepreneur directly from the experts.

When you have a partner or a good friend in life, experiencing success is even better when you can share it. And when you feel failure or have a loss, the pain can be lessened. So when I came across this story we're gonna hear about today, I thought it was important to bring both business and life partners onto the show to tell us about it from both of their experiences. I'd like to welcome to the show husband and wife, Mailynne...I should say wife and husband, Mailynne Calvin and Christian Calvin, as they appear on the screen, both investors and partners in the brandable domain name marketplace named PlentyOfBrands.com. Welcome, Mailynne and Christian.

CHRISTIAN CALVIN: Hey.

MAILYNNE CALVIN: Hi.

MICHAEL: And so you probably recognize Christian, who has been a Sherpa, I think a couple of times on the show in the past. Right, Christian?

CHRISTIAN: Yes, yeah.

MICHAEL: Awesome. Well, it's great to have both of you on for today. Let's jump right into it. What was the domain name that was stolen from PlentyOfBrands.com?

CHRISTIAN: It was kzra.com.

MICHAEL: So it was a four-letter, which, you know, it has a vowel, so it's not considered Chinese premium. But basically, it's a liquid domain name.

CHRISTIAN: Right, very liquid, it's probably something someone could sell pretty fast, couple hundred dollars.

MICHAEL: Is there something that I don't see with kzra? Does it spell something? Is it an acronym? Or is it just a regular four-letter domain name?

CHRISTIAN: I think it's just a regular four-letter. I don't think the acronym means anything.

MICHAEL: Okay. So this domain name, kzra, was stolen from you. What day was it actually stolen? Do you know?

CHRISTIAN: We think it's July 7, around July 7.

MICHAEL: Right around early July. And when did you notice that it was stolen?

CHRISTIAN: Well, probably a couple of days later. What kind of set me off was whenever I tried to log into my AOL account...and like I was telling Mailynne, I'm kind of embarrassed that I actually have an AOL account.

MICHAEL: Plenty of people have AOL accounts. You're not the only one.

CHRISTIAN: Yeah, it's just I've had it for so long. I mean, obviously, I've got Gmail accounts and I've got the Plenty Of Brands accounts too. So I had the email account, AOL account, and I was trying to sign in from my phone, which usually, I just hit the little...like everyone else, they hit the mail button on your phone, and it pops up your mail. And it kept saying, "Wrong password." And I'm like, "No, wait. Like, my phone knows the password." So that's kinda what started it.

MICHAEL: Yeah. So how many days did you go thinking that, "Oh, you know..." Because sometimes, my internet goes down, or, you know, AOL or some other mail provider is having an issue. So I might just wait today for it to resolve itself. Did you wait a few days?

CHRISTIAN: Well, no, I didn't. I noticed it probably at work at around 2:00 in the afternoon. And, you know, I went about my day. I checked my Gmail,

checked every, you know, regular mail I had. And then went home, ate dinner. And then I kinda relax, and I work on domains. And that's kinda when I said, "Hey, I need to get into my AOL account." Got my computer out, could not log in on my computer. So I thought if there was a problem with my phone, that's fine. When there's a problem with my computer, I'm like, "Wait a minute, I know that my computer had my password on it." So that's kinda what set it off. So I'd say it's probably late that night. The next day, I found out about the domain.

MICHAEL: Okay, so how did you find out about the domain?

CHRISTIAN: So that night, my main goal was just to get my AOL account back. So while I was on the phone with AOL trying to get it back, I logged into my GoDaddy account where I have, you know, roughly 1,000 domains there. And I couldn't get in there. So then I'm like, "Wait a minute. I can't get in AOL and I can't get in GoDaddy. There's a major problem here." So that's when I kinda did the fast track. And I think that night I stayed on the phone till, I don't know, probably, like, 1:00 or 2:00, maybe.

MICHAEL: Oh, my gosh.

MAILYNNE: [inaudible 00:04:18] late.

CHRISTIAN: It was late, but so...yeah. The problem with it is that...and we can get into this a little bit further, is that whenever I call AOL, I couldn't even identify myself, because everything had been changed. Where I was born, my birth date, my phone number, everything was changed. So not only could I not get into AOL to reset things, I couldn't get into GoDaddy either, because some other things like two-step authentication and other things were already set up to a different number. So I'm locked [inaudible 00:04:50] both accounts. So my main goal that first day was, "Wait a minute, I've gotta get this under control."

MICHAEL: So you probably didn't even know that the domain name was stolen, at that point, because you didn't have access to your AOL account, and you didn't have access to your GoDaddy account, right?

CHRISTIAN: Right. And I'm not sure if this is true or not, but I don't even know if you can check what's been...or not transferred, but what's left your account at GoDaddy. I'm not sure. So I didn't know if 1 was stolen, 10 was stolen, or 50. I knew that when I walked in and I had close to the number, it wasn't like 50 names...or, I'm sorry, [inaudible 00:05:31] names. It was between 1 and maybe 30 or 40, because I had a good idea of how many I had.

MICHAEL: So spending all night on the phone with AOL and GoDaddy, did you get control of both of those accounts that evening, or did it take you more than that evening to get back control?

CHRISTIAN: I'm pretty sure I had control of both of those accounts that night. I just didn't know the damage of what was stolen. I actually had no way of checking. I mean, so the name was gone, so GoDaddy, when I called them back, said, "Hey, let's see how many names have left your account this month, and then let's see if you did it." So we looked at the list of what had been moved from my account and whether I sold a name or...you know, those were gone. But as far as this one particular domain, I said, "Hey, that's been stolen."

MICHAEL: All right, but when you actually got on the phone, you went through everything, you verified what you had sold. But there was still one domain name, kzra, that was unaccounted for, meaning you didn't transfer it, you didn't sell it, but it was out of your account.

CHRISTIAN: Right. And so the nice thing about it is that they can tell me which domains...so all my domains are locked, so they can go back and see the history of what was locked, what was unlocked. So he had other domains in mind, or she, but they just took that one.

MICHAEL: Yeah, meaning the thief, the hacker.

CHRISTIAN: Right.

MICHAEL: Took only one domain name.

CHRISTIAN: Took only one, yeah.

MICHAEL: So you went to bed at like 1:00, 2:00 a.m. that evening, and you had control of your AOL account and your GoDaddy account, but one of your domain names was stolen. How did you feel?

CHRISTIAN: Well, I mean, I felt really bad. I mean, you know...I mean, I work hard for the domain names. I mean, you know, I need the domains. You know, we have a family, we have children, and we look to...I mean, obviously domaining is a hobby too. We're investors, we like buying, we like selling. But, you know, it's like anything else that's stolen from you. It kinda hurts. And at that time, I did not know that there was any domain stolen. I didn't find that out until, like, a day or two later when I called back to GoDaddy.

MICHAEL: [inaudible 00:07:53] call back to find out. You didn't find out that evening.

CHRISTIAN: Not that evening. So that evening, I just wanted to get control of both accounts, the AOL and the GoDaddy account. Then it was a day or two later when I said, "Wait a minute," you know, "let's check it." So I called back in, and that's when we found out that there was a name that was missing.

MICHAEL: Yeah, and what was Christian's mental state at that point, Mailynne? Because I remember...you know, I'll preface this by saying I remember when I was going to school up in Berkeley, and I left for the weekend to, I think, go hang out with my now wife and came back, and my entire apartment was burglarized. They stole my computer, they stole...you know, they took off the pillow case from my bed so they could put stuff in it

as they carried it out. It was the worse feeling. I felt violated, you know, really, and a little unsafe that somebody had come into my house and taken something. And so I can only imagine, like, did that make you feel the same way? What was your impression, Mailynne?

MAILYNNE: Well, Christian was pretty mad. Domains are like his baby, so he's pretty protective of them, and whether it's good business or not, sometimes he's emotionally attached to them. And then I, also being protective of him, feel bad. And it's not the same as being physically burglarized, but you do feel violated and a little bit scared of your security, because so many things are online these days. So that has been definitely in the back of both our minds [inaudible 00:09:26].

MICHAEL: Yeah, definitely. So it was a couple days later, you called up your GoDaddy rep, you determined that kzra.com left your account without your permission. Did the hacker thief, even contact you by that point?

CHRISTIAN: No. No, there has been no contact.

MICHAEL: No contact. So then the next thing that you did was try to get it back, right?

CHRISTIAN: Yeah, I mean, the very first thing I did was, "Hey, let's look up the WHOIS on kzra.com." [inaudible 00:09:59].

MICHAEL: Yeah, and what did you find?

CHRISTIAN: And it was in Christian's name, and now it's in someone else's name. So, obviously, you know, we're not gonna name any names on that. We don't know if that's a real person or if it's a made-up name or anything. I don't know. But, you know, the goal was to get the name back. It's like, "Hey, how can we get the name back?" So I talked with some people, and then I thought, "Well hey, you know, this is a theft case, possibly. Let's contact an

attorney. Let's see what my, you know, options are as far as that." So that's when I called David Weslow.

MICHAEL: Okay. And David Weslow, of course, is an advertiser, sponsor on DomainSherpa, so you've probably heard his name in the past.

CHRISTIAN: Yeah, and when I first called him, I'm like, you know, "Have I met you before [inaudible 00:10:47]." He's like, "Hey, I've been in Names quite a few times. I don't think we've actually met. Unfortunately, we're meeting with this, you know, bad circumstance." And so that's kinda how we led it off. And he had said he had watched my show, so we knew of each other, so that's kinda how it started. And then from there, basically, I just wanted to talk to him about, "Hey, here's what happened. What are my options, and can we do anything about it?" You know, and it's not covered under, I guess, a UDRP, so...

MICHAEL: Because you don't have a trademark, and UDRP law covers trademarks as they relate to domain names.

CHRISTIAN: Right. So that route would have been much less expensive, I guess, if we're just talking about a pure cost of getting the domain back. Yeah, I felt pretty confident that after speaking with him, I'd be 100% sure I'd get the name back. But then it's like the cost issue. So we have to look at what's the value of the domain versus the cost of getting it back. And this is something that her and I discussed, because it was quite a bit of money, because it had to be handled through a federal court system, which there's paperwork filings, there's meetings, there's all kinds of things that I'm sure that Mr. Weslow would have to do on our behalf. And that's not cheap.

MICHEAL: So you couldn't do the UDRP filing. He suggested you could go to court and file a lawsuit to lock the domain name and get it back, but it's gonna cost a certain amount of money. Did he give you a ballpark how much it would cost?

CHRISTIAN: Yeah, so it would be around probably $15,000. So when we found that out, we're like, you know, "Okay," so at this point, we're thinking, "Let's just write this domain off. It's not that important." See, the thing is, is you have to, at that point, weigh in he's taken money from our family and our...you know, as far as a name. I mean, like [inaudible 00:12:39] liquid. I could sell it right now for $300 to $400. That's just a liquid domain. Is it worth a lesson to teach somebody that that's bad, to pay $15,000 to get it back? Him and I both agreed that it's not. Now, if it was like...floor.com is using the domain, something that's [inaudible 00:13:02] millions, then $15,000 is a very small price to pay to secure the name back. So with it being a four-letter dot com and it's not, you know, something like eBay or Soho or something like that, we decided, "Hey, it's gone." Like, "Let's just move on."

But within that conversation, Mr. Weslow suggested one important thing, he said, "Hey, why don't you email it?" You know. So, at that point, I was like...obviously, I was thinking, "That email address is not gonna get any life."

MICHAEL: Yeah, surely the WHOIS information that this hacker thief put down on the domain name when they transferred it was fake, right?

CHRISTIAN: Right, yes.

MICHAEL: But you tried it, you emailed.

CHRISTIAN: I tried, and...look, I tried, and then I didn't hear nothing for three days, and like I said, it's just a gone, and that's fine. Because, at that point, we pulled up Efty, and looked at...and what I love about Efty is I can see what I paid for the domain, when I bought it, and what my investment was in it, and how long I've had it smudged up. So I pulled it up and noticed that, you know, I had less than, you know, 400 bucks in it. So it's just a $400 lesson, and we kinda just said, "Hey, that's fine. That's how it'll be." So we weren't gonna pay $50,000 to get it back, and...you know.

MICHAEL: Yeah, if you paid $10,000 for the domain, you might think about it, or you would probably do it, right? I don't know. Would you, if it was a $10,000 purchase and $15,000 to recover it, and you had a pretty good chance of recovering it since it was stolen?

CHRISTIAN: Yes, I would, because if I bought a domain for $10,000, I'd be thinking it's a $100,000 domain [inaudible 00:14:46].

MICHAEL: Okay, so it's the retail value. What was the retail value on kzra.com? What would you sell it for if, you know...well, you do own it again. We'll get to that, but what's your retail asking price on it?

CHRISTIAN: Well, so I had it listed, actually, at Plenty Of Brands, and it's probably still pointed there, I'm not sure. And I'm just gonna guess, I don't know exactly what I have it listed there for, but it's probably around $1,600, maybe, I'm thinking. But I don't know. Like, somebody could pull it up and see it's $4,000 or something.

MICHAEL: Yeah, somewhere on that order of magnitude, though. Yeah.

CHRISTIAN: If that happens, and we all know it's not a $4,000 or...but to the right person, it could be worth that.

MICHAEL: It could be. It could be, you know, the initials of a law firm. Who knows, you know? And they wanna shorten to it. That's the beauty of these types of domain names. You've got the liquid value today for other investors, but then you could have a retail value of it in the future if, you know, a highest and best use case comes along. So you emailed the hacker thief and you actually heard back.

CHRISTIAN: Yeah, after about three days, he responded back. And, you know, it kinda caught me off guard [inaudible 00:15:55].

MICHAEL: Yeah, what did he say?

CHRISTIAN: I was like, "What's going on here?"

MICHAEL: Well, first of all, what did you write to the hacker thief? We'll just assume it's a "he" for lack of knowing. What did you write to him? What do you put in an email to somebody that steals a domain name from you?

CHRISTIAN: Actually, it was just honest. I said, "Hey man, look, I want the domain back. I think that you need to return the domain. I have mouths to feed," you know? The way I was looking at it is if it's okay to steal this, it's okay to steal a more valuable domain. So I don't think any theft is okay. So I just said, "Hey, you know, I'd like to have the domain back. Please give it back. I have mouths to feed." And his response was, "I do this because I have mouths to feed," or something of that nature.

MAILYNNE: Well, he was text messaging you from an email.

CHRISTIAN: Yeah, he was text messaging me and, you know, he was like, "Look, prompt responses is what you need to do. We need to settle the..." you know, and then that's when the language on the blog post of Plenty Of Brands where I kinda outlined the back and forth was he wanted to get paid for the domain to give it back. And, you know, it's a lesson, and I probably would pay a certain amount for the lesson of it, maybe to learn. But as far as getting the name back, I just kinda didn't wanna pay for that.

MICHAEL: Right.

CHRISTIAN: That's mine.

MICHAEL: And so when he got these text messages back, Mailynne, was Christian mad? Was he shocked? Was he surprised? What was, you know, going on at the dinner table discussion around, you know, discussing this domain name with a thief?

MAILYNNE: So we were actually traveling, and he was mad. I was surprised. I just assume that people are good, and I was super surprised that someone would steal something and then try to sell it back to that person.

MICHAEL: Yeah.

CHRISTIAN: That's what was so...she was totally surprised with that. She's like, [inaudible 00:18:06] about that. She's like, "I cannot believe this guy's holding your name and trying to sell it back," which I figured that's the only reason why he did it. She's like, "I can't believe this."

MICHAEL: Yeah, I tend to think people are good, as well, and it's always shocking when, you know, somebody's willing to, like, come up, pick my wallet out of my pocket and then offer to sell it back to me for, you know, money. It's ridiculous. And so did this back and forth with the thief sort of kill the vacation?

MAILYNNE: Well, we were on the way home, so it was fine.

MICHAEL: Good.

CHRISTIAN: We were already mad having to leave. We're like, "Man, we don't wanna leave this place."

MICHAEL: So how did the hacker start text messaging you? How did you go from an email to a text message?

CHRISTIAN: So that's still to this day kind of like a question I have no idea. Like, the only thing that I was doing was emailing him, and then all of the sudden, I looked down at my phone, it's like, "Hey, prompt responses, can you hear me?" Or, "Can you respond?" And I said, "Yes," and then we started a conversation there. We also communicated through email as well, but we were communicating both ways at that point.

MICHAEL: And so the WHOIS phone number that you had, was that your cell phone, potentially?

CHRISTIAN: Yes.

MICHAEL: Okay. So he probably just sent a text message and then wanted you to respond to confirm that it was a cell phone, because when he sends the message, he doesn't know if it was delivered or not.

CHRISTIAN: Right.

MICHAEL: Okay, so you went back and forth with this hacker thief, and how much did he want for returning the stolen domain name to you?

CHRISTIAN: So going back to the value of what I have it on there, maybe I did have it at $4,000, because I think his initial response was, "Hey, you can have back for a fourth of what you have it listed for," for $1600, I think. So I guess I did have it priced at about $4,000. But, at that point, he basically, that's where he was. And I was like, "No, I'm not paying $1600 for that domain back." So that's kinda where we started. Then he went down to $600, then he went down...you know, and then he started coming down, down. "No."

MICHAEL: So you basically just flat out refused, and then he came down in price.

CHRISTIAN: Yeah, and he kept coming down, coming down, coming down. And then, at some point, I was like, "You know what? It may be worth something to learn how he did it [inaudible 00:20:43]..."

MICHAEL: Well, before we get to that, Christian, you made a post on PlentyOfBrands.com on the blog area. And I believe that post was July 27 that you made that, if I'm remembering correctly?

CHRISTIAN: I think today's the [inaudible 00:21:00].

MICHAEL: Yeah, you're right. Today's the 27th. You made the post a few days ago.

CHRISTIAN: Yeah, 23rd.

MICHAEL: The 23rd. And then what did you say in that post, and why did you make that post?

CHRISTIAN: So the main goal...and this is where my wife is a big help, she came in and she's like, "You know, this is the type of thing that you probably need to get out there," because I'm the type of person it's like I'll just move on to something else. I'll be done with it, they can have it, they can sell it, whatever. She's like, "You know, this is the type of thing you need to make a blog post about, and you need to let people aware of it." So, obviously, if you look at my website, I'm not a blogger. I don't write a lot. You know, obviously, if I've been on the Sherpa show, if I've done something in the industry, I'll put it out there. But I'm not an active blogger, like, every day or anything. So this was actually a good time to do it, because if I was gonna do it, it's a big enough issue that I felt like, "Hey, there's gonna be some people read this thing. So it's important to know that it was a stolen domain."

So Mailynne suggested, "Hey, let's write a nice blog post and let's let people know what happened, and let's even show them some communication." So that's kinda what we did, so we basically wrote that post that night. And it let everybody know what happened and that this is a real thing, that this can happen to others. So the main goal was, "Let's get it out there, let's let other people know that this can happen."

MICHAEL: Yeah, and then from making that post and telling people the domain name was stolen and sharing some of the communications back and forth between you and this hacker thief, Theo over at DomainGang.com saw that it was stolen. And he's had a lot of experience with stolen domain names

and helping people recover it or getting the word out. What happened when he saw the blog post?

CHRISTIAN: Yeah, I actually think that he's a big reason of why I got the name back. So I really appreciate what he did. He read mine and then reached out to me through some messaging and showed concern, which, you know, we're both blown away by the concern that people have showed in the domain industry. It's really awesome. So Theo's a very nice guy, a very knowledgeable, a very sharp guy. He put a blog up himself, just a simple post like, "Hey, so the domain went to NameSilo. So his post was "NameSilo, do the right thing." And I think that woke some people up, because our blog posts were not necessarily followed by a lot of people. We don't have a big following of our blog or anything like that. Him, Theo, on the other hand, does. And when he put the word out, things started happening. So I feel like that was a big part of helping get this name back.

MICHAEL: Yeah, and so you actually had conversation with NameSilo before Theo, you know, picked up the baton and started to run with it as well. So let's back up the story a little bit. You reached out to NameSilo to try and get the domain name back, right?

CHRISTIAN: Yeah, yeah. So, I mean, as soon as I looked up and saw that the domain was at NameSilo, I mean, I'm like, "Hey." And after speaking with an attorney and some other stuff, I'm like, "I can try to reach out to them and try to see, hey, let them know what happened, then see what they wanna do about it.

MICHAEL: Yeah, and so how did you reach out to them, by phone, by email?

CHRISTIAN: So, by phone. So I called the phone, and, you know, I don't have any names with NameSilo, so because I'm not a customer, I don't know if I was treated this way. I mean, I'm not trying to bash any company or anything. They were not very nice, very helpful, or anything. You know, the guy that I talked to actually said, "Hey, you know, just yesterday or last week,

I had a guy call and say that he had a domain stolen, and he was the thief." So somewhere in this conversation, I was like, "Wait a minute. I'm trying to, like, talk to you about my domain, getting it back, and this guy saying that I could be the thief." I'm like...

MICHAEL: Well you know, yeah, you've gotta feel badly, because the domain was stolen, and you're like, "I just wanna try and get it back as soon as possible before it goes any place else." And you wanna be believed, right? Because you are the victim in this case. But I totally understand where they're coming from, because they probably have a lot of people trying to social engineer and steal other people's domains by getting access to their account. So they need to look at anybody that's calling up saying, "Hey, I need this domain name back" with a little bit of, you know, grain of salt in trying to figure out what's real and what's not real. But they should have an escalation process, so they should have some sort of way to figure and, you know, do some research on it. That's their business, right?

CHRISTIAN: Yeah. There was no escalation. There was, like, no "Get off the phone. We don't wanna talk to you." And, you know, like I said, I kinda understand where they're coming from if somebody just calls up and says, "Hey, you can look and see the domain was just in my name a few days ago, and now the domain's in this person's name. Then you start looking at 'Is this his only name? If that guy had 500 domains, then wait a minute, I could be the person calling in.'" But if this guy's got, like, one or two, and he just started his account yesterday versus calling, maybe, GoDaddy and digging deeper. I think they just didn't wanna spend the time on it.

MICHAEL: Yeah.

CHRISTIAN: I guess I can understand that. And then I also think they don't...I just told them, basically, you know, "You're basically [inaudible 00:26:56] the stolen merchandise. I mean, you have a company, the domain is stolen. I'm letting you know it's stolen, and you have it. So we need to do something

about that." You know, and I mean, I was very nice. I mean, I tried to be nice. I just think that they didn't want any part of it, you know?

MICHAEL: Yeah, did they give you any advice on how to try and get it back? Did they suggest, you know, "We can't initiate this kind of thing, but if you go to GoDaddy and they, you know, do the research and realize it was stolen and contact us directly, then we can start something"? Did they say anything productive, constructive, useful like that to you?

CHRISTIAN: They did say something that was very important to me. They said that when they look at transfers, they look at whether or not it's ICANN approved, or if it follows all of the guidelines of ICANN. So let's backtrack to when he stole my email and when he stole the domain. So he had control of my email, and then he also had control of my GoDaddy account. So when he wanted to transfer it out, he would just go to AOL and approve it and then transfer it through. So, when that happened, everything was followed the way it was supposed to be through ICANN.

MICHAEL: But that wasn't really helpful, actually. He's just saying, "We follow all the rules," and you're saying, "The rules were broken, because the thief stole my accounts." And he didn't provide anything useful to say.

CHRISTIAN: No, I mean, at that point, like, I didn't know that it follow the ICANN. I was like, "Wait a minute," you know? "Wait a minute, I don't think that can follow it when it's not even his account." And I thought there were ways of figuring this out, like looking at GoDaddy to see when my account passwords were changed, and "Let's look at this account. Let's look at what..." Oh, so the same thing, you know, [inaudible 00:28:53]...

MICHAEL: So NameSilo doesn't have access to the GoDaddy information. They can't see, necessarily, you know, who had access to your GoDaddy account, that all your password and, you know, questions about you were changed. But GoDaddy should have that in their logs, right?

CHRISTIAN: Right, they did.

MICHAEL: Yeah, so did you go back to GoDaddy and say, "Hey, clearly, you've gone in and seen that my account was compromised. Can you get the domain back for me?"

CHRISTIAN: Yeah, so throughout this whole process, GoDaddy was emailing me. And the communication was through email most of the time. It was, "Hey, we're trying to get the name back. Give us a week. And we're [inaudible 00:29:32] contact with NameSilo to try to work this out." And then, you know, a few days, "Hey, we have an update. They do have the domain, but it followed all the rules, so they're not gonna give it back."

MICHAEL: Really? They said they're not gonna give it back even though GoDaddy told them it was stolen out of your domain account at GoDaddy?

CHRISTIAN: Yeah, they were not giving it back.

MICHAEL: Huh.

CHRISTIAN: So that's when we did the blog post. So this is where it all kinda comes together. So apparently, I guess, I don't wanna say, like, the higher-up type of people in GoDaddy and NameSilo both got ahold of our blog post and Theo's. So that very next day after they read them, that's when everything kinda come together, like, "Wait a minute, we don't want our name attached to the..." you know...

MICHAEL: Right, yeah. Imagine that, some bad press is coming out of not standing behind... Well, to NameSilo's point, I guess you're not a customer there, you don't have any domain name, so it's GoDaddy's obligation to try and satisfy you as a client to try and get that domain name back.

CHRISTIAN: And they did, and then I heard from GoDaddy, and GoDaddy said, "Hey, we have some good news. Now, at this time, I already had the name back.

MICHAEL: Yeah. Okay, so let's pause that story there for a second. How did you get the domain name back from the hacker thief?

CHRISTIAN: Okay, so...well, at this point, I'm thinking, "I may pay something for this back. Like, I may actually pay a couple hundred bucks for the name back..." or not for the name back, but for information of how it happened and stuff like that. So I wanna know how it happened, how I can prevent it from happening, and pay for that.

MICHAEL: Right, because if you just get the name back, you still have a question in your mind, "How did the hacker get into my account? I wanna try and figure out what the root cause was. Otherwise, it could just happen again tomorrow."

CHRISTIAN: Well, and also, I didn't wanna send him money without having the name back. So my first goal was "Give me the name. Like, let's be clear here. I'm not the one that's, like, not trustworthy." Like, "I'm not gonna give you money and then you not send my name, and then you're laughing again," you know?

MICHAEL: Right, because how did he wanna get paid?

CHRISTIAN: He wanted to get paid...well, so probably through something like Bitcoins or [inaudible 00:32:05].

MICHAEL: Right, it's not traceable, it's not trackable. It's an anonymous, you know, currency. You send the money, there's no way to get the money back.

CHRISTIAN: It's gone. So I at first kind of said, "Hey, there is a certain price I wouldn't mind paying. But I need the name back."

MICHAEL: Yeah, and what did he say?

CHRISTIAN: He said, "No, pay me half and then pay me the rest after you get the name back." And then that's when I said, "No, I'm not paying nothing. I'm not paying nothing until I have the name back."

MICHAEL: Was he pretty pissed, Mailynne?

MAILYNNE: Yeah.

CHRISTIAN: I mean, look, at this point, I don't care. Like, I don't care if I get the name back at this point. You know, I was without it for three weeks. I'm like, you know, "You're gonna give me my name back before I pay anything."

MICHAEL: So that's what you're sending him over text message, "Give me the name back before we discuss any payment."

Quick message from three of our sponsors that helped make this video, show, and podcast possible.

First, if you're buying a domain name from a private party and want to know what else they own, domainIQ.com is the tool you should be using. View their entire portfolio, filter by Estibot value and be a better investor. $49.95 for 250 queries per month. Visit domainIQ.com/portfolio to learn more.

Second, Efty was built by domain investors to increase your inquiries, sales and profit. Forget spreadsheets and archived emails — manage your entire investment portfolio in one place using a secure and completely confidential platform. Learn more at Efty.com, that's e – f – t – y, Efty.com.

Finally, if you're struggling with how to buy, sell, and value domain names, you need to check-out DNAcademy.com. Published by me, Michael Cyger of DomainSherpa, and trusted by Uniregistry to train their new employees, you

too can learn using the DNAcademy accelerated learning system for domain name investing. Learn more at DNAcademy.com.

MICHAEL: So that's what you're sending him over text message, "Give me the name back before we discuss any payment."

CHRISTIAN: Right.

MICHAEL: And so did he? Did he actually just give you the name back?

CHRISTIAN: So he did. He actually sent the name back. I created the NameSilo account like he asked, and he said, "I'll just push it into your account." So [inaudible 00:33:14].

MICHAEL: Right. Because of the ICANN 60-day lock rule, once the domain name transfers over from one registrar to another, it's locked for 60 days, right?

CHRISTIAN: Right, right.

MICHAEL: That's a good rule. That's why the rule was put in place, to prevent theft from moving to NameSilo and then suddenly going around the world to a registrar that doesn't necessarily work well with other registrars and could care less about if it was stolen or not. And so he knew he couldn't move it for 60 days from the time that it came in.

CHRISTIAN: Right, and yeah, and I think that's why he just went ahead and pushed it in. He's like, "Hey," and believe it or not...well, I think NameSilo could push it back to GoDaddy if they wanted to.

MICHAEL: They could, yeah.

CHRISTIAN: I think they can. I don't think they want to. But, matter of fact, I know that they want to, because I've had quite a few conversations with

them about that. Because I want it back where it belongs. But, yeah, he actually did push it back into my NameSilo account.

MICHAEL: He created the account, he pushed it over to your account, and then what did you say to...like, you didn't want just the name. You weren't willing to pay him just for the name, you were willing to pay him for information on how he did it, right?

CHRISTIAN: Yeah, and at this point, I want information. And so he was very vague with the information. He wasn't really giving me in depth of how he did it and what he did, so that went on for probably a few days, because...and that's actually still going on. He just has not really satisfied the "This is what happened, this is what you need to do." Because even as we talk right now, he could be doing something. I don't know that. I don't trust him, you know.

MICHAEL: He did give you some information, right? He told you in general terms what he did, and you and I have chatted about it a little bit what I think has happened. So, you know, and this is the frustrating thing, is as I said in the intro, I hear about a lot of domains being stolen. I can never get to the root cause of how they were stolen, how they got access to the email account, how they got into the GoDaddy account. But you asked him, "How did you do it?" And you may not have the whole story yet, but we can sort of deduct some things. And what did he tell you about how he did it?

CHRISTIAN: Well, he said that he comprised, obviously, my AOL account first and then compromised my GoDaddy account after that. But how he got the information was through, like, a LinkedIn data set breach. So I Googled...I mean, obviously, we looked that up, and that happened in, I don't know...

MAILYNNE: In last spring, actually.

CHRISTIAN: Was it?

MAILYNNE: It was in 2016.

CHRISTIAN: So it was in 2016 this happened, and I guess there's things out there that are just scouring the web just to try to grab usernames and passwords.

MICHAEL: Yeah, so plenty of large sites have been hacked, and their databases of users have been stolen. Dropbox had it, Yahoo had it, financial institutions have had it, and LinkedIn was one as well, exactly how you mentioned, last spring 2016. There was a file, 167 million email addresses and passwords were stolen. But way back in 2012, they were stolen, but they just weren't offered for sale into the dark web, you know, the seedy underbelly where drugs are sold and things that are illegal are sold. And so what had happened is this hacker had the database, offered it for sale for basically $2,000. And he sold it a number of times. And usually, a database isn't that bad. Like, you'll get the email address, but you won't get the password, because it's protected. You know, people call it salting and hashing, where you actually obscure the password and so people can't find out what the...it's not stored in a regular ASCII text.

But LinkedIn, back in 2012, didn't do salting and hashing. They only hashed it. And so, basically, the underworld just cracked all the passwords for these 167 million email accounts. And, you know, a lot of us, myself included, up until just a year or two ago were very complacent with our security. You know, we create very in-depth, intricate passwords that have numbers and letters and capitals and special characters and things like that. And we think we're safe, but then we go and we use that same password everywhere, because, you know, how are we supposed to remember crazy passwords like that, right?

CHRISTIAN: Yeah. You're right, I mean, that's the thing is that, you know, a lot of the areas we had is similar or the same. And he actually told me my passwords. He actually emailed me and told me [inaudible 00:38:15].

MICHAEL: So he told you the password. And that was the password that you had...and I asked you, I said, "Was that the password you had for LinkedIn and the password you had for AOL?"

CHRISTIAN: And we checked it out, and yes. So that makes sense. And, you know, I mean, like I said, I don't know who this person is or what they do or if they sit around all day and try to figure these things out and they're good at it. But, yeah, I could have been very easy.

MICHAEL: Yeah, and so, you know, you think about it, and if you're a hacker and maybe there's not work for you in whatever part of the world that you live in and you're doing this thing, like, you have the email address, so you know it was an AOL account. And then you match it with the domain WHOIS, and as investors, we want our email addresses to be public so people can contact us. And if you're using an AOL account, why don't I just try and sign into that email address at AOL using the password that they have in LinkedIn and see if I can get in. Now that you're in...you know, your email is basically your life blood of your life, nowadays, right? We use email for everything.

CHRISTIAN: Well, I think at that point, you can go to, like, a place like GoDaddy and see that my names are through my AOL, and then reset the passwords and get the password reset to the email. And then change passwords, change two-step authentication, change some things which lock me out.

MICHAEL: Right. Yeah, it's amazing that you only need...you know, you can reset your AOL if you're into AOL. Then you can reset your password at GoDaddy. And then, to update your security questions, all you need to do is know the password, right? So it's sorta...

CHRISTIAN: [inaudible 00:39:58] in changing them, yeah.

MICHAEL: It's not really security if all you need access to is your email account at AOL.

CHRISTIAN: Right. And yeah, so I think if I had all of my domains...and kinda the lesson I've learned, and I don't know if this is true or not, but if I had, like, a Gmail or something instead of an AOL, so I may have used a different password there, possibly, I don't think any of this would have happened. And especially with Gmail having, like, two-step authentication, or two-factor authentication, or whatever they [inaudible 00:40:32], that it would have probably stopped all this from happening. Now, GoDaddy is still looking at how this happened, because they even have steps beyond just the normal things to stop things like this from happening. So they're kinda reviewing of how this happened.

MICHAEL: Right, like I would have thought that GoDaddy, before a domain transfers out of your account, maybe they should verify...well, I was gonna say the IP address, see if it's a different part of the world.

CHRISTIAN: Yeah, I mean, I think they could do stuff like that.

MICHAEL: But they sent the email address to the AOL account, and so, you know, theft is probably a very, very small, insignificant portion of the number of domain transfers that happen every day.

CHRISTIAN: Yeah, and I think that they have this thing, it's DTVS, it's like domain transfer validation service, and it's a very, what I would consider secure way. You actually have to talk to someone before a domain leaves my account. So I have that set up on my account. I'd sold probably, you know, four or five domains in March, turned it off, because I was needing to transfer these all through there. Then, I'd been busy with work and some other things, didn't turn it back on, which, if I'd have just had that on, this wouldn't have happened.

MICHAEL: Yeah, so it's basically an extra step to the process. DTVS is exactly how you described, and it's for premier accounts. So, you know, the way GoDaddy explains it to me is that if you spend about $5,000 per year on all

products at GoDaddy...you know, it could be just domains, or domains and hosting, or domains and SSL, whatever, you can get access to a premier account rep, and then they can turn on this DTVS. And basically, they will call you...whenever you place a transfer or somebody else places a transfer, they will call you on your cell phone or home phone or whatever, and then ask you for your pin number and then verify, by voice, using your account rep, that you actually wanna transfer that domain, right?

CHRISTIAN: So if I'd have had the DTVS, obviously, my account rep would have been like, "Wait a minute," you know. Even if they changed the phone number in my account when they call, my account rep and I are pretty close, and we talk fairly regularly. And he knows my account, he knows my domains, he knows what I do, so he would have put a stop to that pretty quick. So [inaudible 00:42:56] DTVS would have stopped. Obviously, two-step authentication and DTVS is kinda going overboard, but when it comes to your investments, maybe it's, you know, okay.

MICHAEL: Yeah. Well, I can tell you I do have DTVS turned on on my account too, and it is kind of a pain when you, like, put in the transfer or, you know, the buyer puts in a transfer, and then they text you or email you later in their day, and they're like, "Hey, I didn't get the domain yet." And you're like, "Oh yeah, nobody from GoDaddy has called me," right? Because it goes through their internal process, then your customer service rep needs to see it in their queue, and then they need to call you when they have time. And if they're not in the office for whatever reason, then somebody else needs to pick it up, and that could delay it by a day. But you can go and call and ask to do it, and then they'll call you back and run through the, "Hey," same process. But it takes time, right?

CHRISTIAN: Yeah, I mean, I think it's about 24 hours. So let's say I sold a domain for, I don't know, $8,000 to $10,000. That person wants that name. They've already paid, they want that name. So sometimes, I'm just straight up honest and say, "Hey, this process is gonna take a couple of days, let's just be

patient." If I did not have DTVS, it would take five minutes or whatever, just enough [inaudible 00:44:12] go in there and grab it.

MICHAEL: Right, sometimes it's instantaneous, exactly.

CHRISTIAN: Yeah. So it is a little bit slower. And you know, and then again, if someone's gonna send $5 to $10 to $20 to $100,000, what's another 24 hours to make sure it's safe? So, you know, it's a smart thing to have, especially if you have things at GoDaddy. And if you're a premier member, obviously there's certain levels that you have to be at to have that type of an account. They can't do that for everybody. But if you are at that level, then it's a good thing to have.

MICHAEL: Yeah. And I don't remember how I turned it on. Do you remember how you turn DTVS on or off? It's not something that a hacker who gets control of your account can do, can he?

CHRISTIAN: No, it has to be through them.

MICHAEL: Nice.

CHRISTIAN: So I've actually talked to my rep and called. And so, basically what I'm saying is the hacker could not have gotten into my account and turned it off. So that domain would have never left my account.

MICHAEL: Yeah. Okay, so let's say that, you know, most people watching this show probably don't have premier accounts, because they maybe don't have as many domain names or something like that. I do have two-factor authentication hooked up on my account, so GoDaddy will actually text message me every time I try and sign into my account. So basically, I enter my username and my password, and then it comes up with a two-factor screen, and it says, "Type in the number that we just texted you." So the hacker would have to actually steal my phone or steal my SIM card or, you know, some really high level of sophisticated hacking in order to get access to

my phone to then get the number to enter in to sign into my account. So that could have prevented it, right?

CHRISTIAN: That could have prevented it. I think the two-factor authentication would have helped a lot. This particular guy that did it actually kinda indicated that he can get around that too.

MICHAEL: Really?

CHRISTIAN: Yeah, so you know, even as we're talking right now, we don't know what's gonna happen. We don't want it to happen to nobody, you know? It's like, "Look, go do other things," you know? I mean, I don't know.

MICHAEL: Go be productive, exactly.

CHRISTIAN: It's like, leave us alone, please. So I think any time that you have things with your phone or computer, they can be manipulated. And what I mean by that, there's a new type of threat going on with SIM cards, and I think it's like...and I don't know exactly how this works. I'm trying to do a little bit of research on it, but apparently, they can...I don't know if they call in to, like, your carrier and say, "Hey, I need to get a new SIM card," whatever. And then they finally, you know, somebody may actually do it. And [inaudible 00:46:48] do it, and then they can get control of your phone. And then the two-factor comes there and then they're, you know, [inaudible 00:46:53.

MICHAEL: Yeah, so I've been doing a little research on that as well, and that is actually happening where hackers will call your phone company and social engineer their way to get a replacement SIM card. So, you know, if I take my phone out of the case and then look on the side here, that's my SIM card right here, and I can pop it out. And, you know, if I'm a hacker, I get your physical phone, I can pop out the SIM card, put it into a duplicator, and duplicate it, right? But how many times does a hacker from some place around the world get access to my phone? Not very. But maybe they could call and talk to my carrier, like it's happened with some really big YouTube

stars, people with, like, 10 million people that follow them on YouTube. They've figured out the phone number, and then they've called their carrier and gotten a replacement SIM card. And then suddenly, they can now verify themselves to get into the YouTube account and take over that account.

CHRISTIAN: So that's, I think, the threat that, you know, everyone kinda needs to watch for is that whether you're with Sprint or Verizon or whoever you're with, people can call in, manipulate, say, "We need a new SIM card." And then I'm not sure if they actually need your physical phone at that point. I think they can, if they have [inaudible 00:48:10], mine's done. This is the new one, two-step authentication comes here, and then we're back in the same situation. So look, I mean, I think as long as we have valuable assets anywhere, there's gonna be people that are gonna try to take them. You know, I mean, it doesn't matter if it's a vehicle or a property or whatever. I mean, I think that...you know, this is internet real estate, so I think it's a little bit more appealing and attractive to somebody like a hacker, because it's their world that they're in.

MICHAEL: Yeah. So it sounds to me like it could have been prevented, but of course, I'm not gonna say that, because who knows what the hacker will do or what hackers are gonna be able to do tomorrow or anything? But if you didn't have the same password for both your LinkedIn and your AOL account, they might not have been able to get into your AOL account. If you had two-factor authentication hooked up on your AOL account, they may not have been able to get into your AOL account. It was through your email that they were able to get access to your GoDaddy account, because the password reset came to AOL. You know, any changes that needed to happen were notified on AOL. The approval notice for the transfer out of GoDaddy came to your AOL.

So you gotta use different passwords on every single site. They have to be really long, complex passwords, and there's no way to do that unless you use a third-party application like LastPass or 1Password to manage all of them

and have it on your computer and your phone. Does that sound like a fair analysis of that?

CHRISTIAN: Yeah, I think so. And then, you know, her and I were talking that, you know, how secure is LastPass, or how secure is 1Pass? I don't know. I mean, they very easily could hack that and get the...

MAILYNNE: They may have a security [inaudible 00:50:11] that we don't know about.

MICHAEL: Yeah, so the way I understand it is that they don't actually store the information on their database, it's actually stored on your local computer, and it's using, you know, the most secure cryptography that's commercially available today. So I think if a hacker actually got the data file from my computer and tried to hack it, it's so complex that it would take years to hack. That's what I understand. If anybody's watching this show and understands cryptography and hacking better than us, please post a comment below and tell me, if you had access to my one password data file, how long would it take you to hack and tell me the websites, the email addresses, and the passwords? I'd love to know that as well.

CHRISTIAN: Yeah, you may get a message with those that say," Hey, here it is."

MICHAEL: And hopefully, they can never get that, because they're only on, you know, my applications. I don't believe that they're backed up into other locations.

CHRISTIAN: If someone tells you your passwords...

MICHAEL: That's pretty scary, right?

CHRISTIAN: That's a scary email, text message, or whatever when he's like, "Oh, here's your last two." I'm like, "Oh, god."

MICHAEL: Right.

CHRISTIAN: I mean, I think he even had the one before this one, so yeah. I don't know. I don't know how. He said, "This is your last two." I don't know if it was different sites or whatever, but he...I don't know if it was the last two that I'd sent on any website. I'm not sure. Like, I don't know.

MICHAEL: I actually tried to download the LinkedIn stolen database and then tried to undo the caching that was on the password so I could tell you if that was the password. But I actually couldn't find the database any place on the web anymore. I think LinkedIn's done a good job trying to eradicate it, and I didn't wanna go to the dark web, because I read this terrible book about what happens on the dark web, and I didn't wanna see any of that.

CHRISTIAN: So what is that? I don't even know what that is.

MICHAEL: Oh, my gosh. What was the book that I read? I think it was called "The Dark Web" or something like that. Some journalist went underground to interview hackers and people about what the dark web is, what happens down there. There was a whole chapter that I didn't even wanna read, because it was, you know...and the chapter started off, "If you go to the dark web and you click one of the links to go to a certain section, you cannot unsee that." And I'm like, "Yeah, I don't think I wanna see that." So I don't wanna install the special browser that you need to get onto the dark web.

CHRISTIAN: Is the dark web a part of the web? Or is it a whole nother...like, it's just a part of the web?

MICHAEL: It's a part of the web that you typically can't get to...you can't get to it from your Chrome, Safari, Mozilla browser. You need to download a special browser that verifies that it's an anonymous access to a portion of the web where societal norms do not necessarily apply. So if you're cool seeing things that most of us would find appalling, then that's fine. Also Silk Road, where

drugs were sold back and forth, that's a part of the dark web. And that still occurs, so you can buy whatever illegal drugs you want on the dark web, you know, things like that.

CHRISTIAN: Wow. [inaudible 00:53:39].

MICHAEL: You know, Christian, this hacker could have stolen all your domains at GoDaddy, right?

CHRISTIAN: Right, yeah.

MICHAEL: He only took one. Why do you think he only took one domain name?

CHRISTIAN: Well, you know, I'm not sure. He said he had a change of heart. I don't know if he knows me or...like, I don't know. But, you know, I personally think that it would have been pretty expensive. Like, you know, transfers are $9, $10, $11 apiece, and if I've got 1,000 domains, that's like 10 grand. And, you know, my portfolio may not even be worth 10 grand. So [inaudible 00:54:15]. So yeah, I'm probably like anybody else. I've got a few good names and then I've got 900 bad names or [inaudible 00:54:26]. So, you know, I'm not probably, like, the biggest target, because I just don't have a portfolio of, like, one-word, $1 million dot coms. But I do have a lot of...not a lot, but some liquid domains that you and I both know that can be sold right now. And it's not a lot of money, but it doesn't really...it might be to him, you know, like [inaudible 00:54:51].

MICHAEL: Yeah, great point. Like, 400 bucks may not be a lot to us, but if you're in a developing nation, 400 bucks could, like, feed your family for a month or two, or more. Yeah.

MAILYNNE: I think there's a couple of things. It may have thrown up a red flag to transfer out in multiple domain names, so he might have just tried one first.

MICHAEL: Yeah.

MAILYNNE: And the other thing, we've been super grateful that the domain community has really kinda rallied behind us. There were a couple of areas he might have been able to sell it, but at this point, the word was out. So he may have realized he couldn't sell it on those platforms and decided to then sell back to us.

MICHAEL: Yeah, where might he have gone, Mailynne, to sell this domain name, kzra.com?

MAILYNNE: Possibly one of the domain forums or one of the sites that sells different domain names. And after we posted the blog post, other people were fortunate, we were fortunate enough that they posted on those sites that this was a stolen domain, so don't buy it. So there's some communication back and forth with the hacker. After that, he may have realized he can't sell this domain this way, he either needs to sell it back to us and try to get money that way, or to distribute it some other way that I don't know, because I've never been on the dark web.

MICHAEL: Yeah, don't go there. And so, you know, after a couple of weeks where we've had a lot of uproar in the domain industry, and maybe, you know, a lot of...I don't know, sometimes you get into people really fighting about topics that sometimes are important, sometimes are not important at all. It's nice when something bad happens and people do come and get your back, that they do support you, that they send you the emails, that they take what you posted and take it over to namePros or DNForum, or wherever else they took it, and make sure that this domain name can't be stolen, right? Because if some third party, some other newer domain investor didn't...or experienced domain investor didn't know that it was stolen, they may just buy it for 300 bucks thinking that they got a great deal. And, you know, they're gonna lose their money if it ever gets pulled back through NameSilo

and back to GoDaddy, you know, and then one more person becomes intertwined in this terrible situation.

CHRISTIAN: Or bought it for $200 or $300 or $400. I mean, even somebody like me, so.

MICHAEL: Yeah. So, you know, I go back to the very beginning, like, one of the first things you did was make that blog post, and it must have been very difficult for both of you to, you know, write about the situation, which was difficult, having something stolen from you, and then putting yourself out there and saying, "You know, this..." and being a little embarrassed, like, I would be embarrassed if a domain name was stolen from me. And so, you know, but if you didn't do that, then the whole community wouldn't have been able to come together and support you and get the word out and help you get the domain name back. So, you know, thanks for putting yourselves out there, guys, to start with.

CHRISTIAN: Yeah, I mean, obviously, it is kind of embarrassing. I mean, nobody wants that to happen, but then again, I also feel like part of it's my fault, because I had actually let the security lax. I actually was very lackadaisical about my security, my passwords. And, you know, just in our busy lives that we have, it's not a top priority to make sure that someone didn't hack my account. I mean, we've been in the domain industry for probably six or seven years now or something, and, you know, we'd never really thought that this was an issue. But it is a real issue. It's a problem.

MICHAEL: So now that you understand how the hacker got in, what he did in order to steal this domain name, what are you guys doing differently to protect your portfolio and your business going forward?

CHRISTIAN: So, you know, I've set up the two-factor authentication on the sites that I can, I've changed some passwords. You know, and to be honest, I don't actually, totally feel safe and secure with it, but I think there are steps that you can do to make sure that, you know, that it's a little bit more

difficult. So I like the two-factor authentication where if I wanna get into...if I just wanna go to GoDaddy, you know, I have to enter in a code that's sent to my phone before I can even get in there. So, you know, if it's that secure and safe for me, then hopefully it'll deter anybody from doing that. I'm sure there's a lot of accounts out there that are just like mine that are, like, small to medium accounts that doesn't have that.

And I would just suggest to everybody watching, you know, look, your domains are investments. It doesn't matter what type of a person, investor you are. It doesn't matter if you're buying $5 domains or $50,000 domains. It's money that's from that family or that individual that he's had to work hard for, probably, to get. And, you know, there are some steps out there that make it a little bit harder for people to do this. So it took something like this to kinda open our eyes for our investments. And hopefully, you know...you know, like I said, I got a message today, and I don't know how to take it. I don't know what's going on, but you know, he may try doing other things.

And, you know, I don't always feel completely safe, but the whole goal was to just make it a little bit more difficult to happen, you know? And I know that you have viewers that are from all walks. You have them that sell millions of dollars worth of domains to ones that have never had a domain sell at all. Or, you know, I've read where people said, "I just had a $200 domain sell," and they're just ecstatic. And then $200 domain sales may not interest other people that thought, you know, it's like, "Oh, it's only 200 bucks." So my point to this is everybody's portfolio is very important to them, and even to the domain community. I don't wanna see this happen to nobody else, so you know, if those are out there, those safeguards are there to protect you, you know, go ahead and use them. They don't cost anything. And it may take you five extra seconds to log in, but it's worth it, so.

MICHAEL: Yeah, and I know the firs time I set up two-factor authentication and the first time I, you know, did other things like DTVS, it took a little bit longer, you know? It make take you an hour to learn, but it take you an hour

to learn and it only takes you 5 or 10 seconds longer to wait for that text message to come in before you sign into your account. It's worth it.

CHRISTIAN: It is worth it. And, you know, this has been a three-week ordeal. And I actually, you know, think that there's gonna be other things that...I mean, I don't know how to take this person. I don't know if they're a friend of...or not a friend. Obviously they're not a friend. But I don't know if they're, like, a friend on Facebook or [inaudible 01:01:40] like that. You know, in that respect, it's just a little scary, because it's gonna definitely deter the way that I select people who I'm gonna be friends with on social media. I mean, it's not like trying to get as many as you can so you can grow your brand. It's like, "Hey, wait a minute. It needs to be quality individuals." So...

MICHAEL: Yeah, yeah. And I know I get a lot of friend requests on Facebook from people that I have never met who's name doesn't necessarily mean anything to me, right? And they could be fans of the show or something else, but I just don't know them. And so I don't accept, because, to your point, I'm not sure if Facebook is gonna have a vulnerability someday for a hacker to get access to my computer through the browser because I'm signed into Facebook, or...who knows, right? Who knows? You know, I wouldn't expect LinkedIn to get hacked and have all the user database passwords non-properly, you know, secured. So, you know, it's better to be safe than sorry.

CHRISTIAN: Yeah, and I'm just gonna take...you know, I'm not gonna be accepting a lot of those anymore, I mean, you know?

MICHAEL: Yeah. And Mailynne, I heard that Christian got a new Mac, and Macs tend to be less susceptible to malware and things. Is one of your action items to help get him over to the light side from the dark side?

MAILYNNE: I've been preaching he needs to get a Mac for a year now, so he has one, and I'll help him get converted, and I think he'll love it. And it does tend to be a little bit secure.

MICHAEL: And again, it's the exact same thing. It takes you a while to learn. I remember when I left corporate America, I bought a PC and I was using that, and I loved it, and then I wanted to do, you know, some videos for DomainSherpa. And I just couldn't find the right software or whatever, and so I switched over to Mac just for doing videos and interviews and things like that. And I'm like, "I love it. I never have to reboot my Mac, it always works. I don't have to worry about malware as much, because everybody wants to target the masses of PCs. It tends to be a little bit more secure.

CHRISTIAN: Yeah, I'm gonna like it. She's been on me for a long time. I mean, you know. So I went out and bought it, and I didn't just buy, like, the regular one. I have a really nice one. I mean, [inaudible 01:04:01] into it. So it's like, yeah, I mean, it's all cool. It's got, like...I mean, on the keyboard, it's got a section at the top that lights up that you can...I don't know if you've seen the newest ones out...

MICHAEL: I've got it. It's the Magic Bar, yeah.

CHRISTIAN: It's awesome. I just got, like, a $300 HP computer, so it's gonna be a big...

MICHAEL: Yeah, when I connect to you, it shows, on that Magic Bar, your face and the fact that we're connected on Skype. And so, you know. And it's got the fingerprint login, so whenever I wake my computer, I just put my index finger on there and I don't have to type in a password.

CHRISTIAN: That's what I do. Like, so I have got it out and played with it. So yeah, I just touch it and it comes right up. I'm like, "This is the coolest thing ever." So yeah, I'm excited to get into it. Hopefully, it'll help keep me safe.

MICHAEL: Nice. All right, if you watched this show and you have questions, please post them in the comments below this video, on DomainSherpa, and I'll ask Mailynne and Christian to come back and answer as many as they can. And if you have comments about security that we brought up during this

show, or you have some additional thoughts on ways to add security without being too burdensome, please post those. We wanna hear those as well. If you found educational benefit from this show, or simply motivated by what Christian and Mailynne provided to better secure their domain names, please take a few seconds and just post a comment below, or click the Tweet button and thank them on Twitter.

Mailynne and Christian Calvin, thank you for coming onto the DomainSherpa show, sharing the details of your domain name theft and recovery and how you're gonna prevent it going forward. And thanks for being Domain Sherpas for others.

CHRISTIAN: Thanks, we appreciate it.

MAILYNNE: Thanks for helping us.

CHRISTIAN: Thanks for helping us get the word out too, so thanks.

MICHAEL: Thank you all for watching. We'll see you next time.