Understand and Prevent Domain Name Theft - with Dr. Bruce Tonkin

Watch the full video at:
http://www.domainsherpa.com/bruce-tonkin-melbourneit-interview/

In September 2013, an Activity and Hacker Group called The Syrian Electronic Army hijacked the websites of the New York Times, ShareThis.com, TheHuffingtonPost.co.uk, and Twitter.co.uk. This resulted in traffic to those website being temporarily redirected to a server under the attacker's control. If large, established, and high-tech companies like these are not safe from hackers, are our small business eCommerce and publishing websites safe? Is our email safe? If you want to learn what you can do to prevent this from happening to you, stay tuned.

I have three short sponsor messages before we get into today's show.

First, if you have a great domain name and nothing to show when people visit, you're missing out on potential advertising revenue, leads, and partnership opportunities. NicheWebsites.com can build you a site quickly with a price option to suit any need -- but as their tagline says, they don't just build websites, they build businesses.

Second, 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.

Finally, DNX.com is a domain name exchange that uses a reverse auction platform to provide fair market prices for quality domain names that are manually filtered by an experienced broker. At DNX.com, domain name prices drop until someone decides the price is right; but don't wait too long or a domain you love might be purchased by someone else.

All three sponsors have a clickable banner in the upper right hand corner of DomainSherpa.com. Here's your program.

Michael Cyger: Hey everyone. My name is Michael Cyger, and I'm the Publisher of DomainSherpa.com - the website where you come to learn how to become a successful domain name investor and entrepreneur directly from the experts.

As I mentioned in the introduction, one of the websites that was recently attacked by the Syrian Electronic Army was the New York Times. Turns our NYTimes.com was compromised by what is called a spearfishing attack at one of the resellers of the registrar named Melbourne IT. So, I reached out to Melbourne IT to ask them to come on the show, talk about the situation, and help us all understand how we can protect our domain names, websites, and email from hackers in the future.

I am pleased to welcome to the show Dr. Bruce Tonkin, Chief Technology Officer at Melbourne IT. Bruce, welcome to the show.

Dr. Bruce Tonkin: Thank you, Michael.

Michael: Some of our readers have not ever heard of Melbourne IT. Before we get into the details of what happened, how it happened, and preventive measures, let's start with a little background. Can you tell me about Melbourne IT?

Bruce: Yes. Well, Melbourne IT started off at the University of Melbourne, in Australia, back in 1996, and we were the first administrator for .COM.AU domain names. And then, towards the late sort of 1999/2000, we became one of the first registrars for registering .COM domain names. So, we are now roughly the sixth largest registrar in the world with respect to registering .COM and other domain names. We have a high proportion of domain names with large companies, so often, if a large company is attacked, they will come to us for assistance. And since then, we have also branched out into hosting domain name websites and hosting email for customers as well as search engine marketing and other services you would expect from a web services company.

Michael: Great. And I mentioned earlier that you are the Chief Technology Officer at Melbourne IT. What does your role involve?

Bruce: Basically it involves looking after the strategic technology direction of the company. I have been very heavily involved in the development of the domain name industry. I am, in fact, on the Board of ICANN, and have been the Vice Chairman on the Board for several years. And also I deal with sort of major suppliers and major customers, I guess.

Michael: Excellent. And I appreciate you coming on the show and helping us understand, from a technical standpoint, what actually happened. So, before we dig into the technical details so that people can understand it, let's define what the problem is, because I read a lot of stories and in the general media - domain name hacking, domain name theft, fishing. Let's start with: how do you define what domain name hijacking is?

Bruce: I think hijacking is generally considered to be a malicious act by another party to gain control of your domain name. And once they gain control of your domain name, they can redirect your website to another place, and they can even redirect and capture email, although there has not been a lot of evidence of that being done yet.

Michael: Okay, and how is hijacking when somebody takes control of your domain name different from domain name theft?

Bruce: I would say that hijacking and theft are basically the same thing.

Michael: Okay.

Bruce: Although the other scenario I think that happens is there are other ways in which people can lose control of their domain name. So, suddenly, you see your website has gone off the air and you might think: "Someone has stolen my domain name." In actual case, it may simply be that the domain name has not been renewed and the name has been suspended in some form, and then you do have a period of time, typically from thirty, sometimes 45 days to respond once your domain name has been suspended. But after that point, it can actually be given to a new user quite legitimately.

Michael: Yeah, and I think that case actually happens to more people than theft/hijacking, where a domain name actually just expires. I remember that happened to me back in 2005 or 2006. I had a website that was a publishing company that was generating a lot of traffic, a lot of revenue, and suddenly somebody sent me an email or called me and said, "Hey, your website is not working," and I typed in the address and went there, and it went to a parking page. And back in those days, I did not know what a parking page was, so it was just a listing of ads, and I was like: "Somebody stole my website!"

Bruce: Yes.

Michael: Your brain goes in all different directions, and so what had actually happened is I was negligent and missed one of the renewal emails and my domain name expired. And so, that, I think, I just want to clarify, because you bring up a great point that negligence and letting your domain name expire is different from a malicious act of a third party to take control of your domain name.

Bruce: That is right, and the best way to protect yourself on the renewal front: most registrars now allow you to set the domain name up to be an auto renew. And typical domain names, you can register them from one to ten years, but a lot of people just register them for one year because it is less cash upfront.

Michael: Right, exactly.

Bruce: But if you are going to do that, then you should set it to an auto renew and leave your credit card on file, because then it will just automatically renew. You could always cancel it, so it is not like you are locked in, but it is good to have the safety net of knowing that it will automatically be renewed if you are on holidays, etc.

Michael: So, how frequently does domain name theft happen, Bruce? Are there any statistics about that? It seems like there is a rash in the media outlets nowadays, talking about domain name theft, but how frequent is it?

Bruce: It is not very frequent. Well, I mean we have sort of, I guess, three to four million names under management. We might see the equivalent of an incident probably once every few months, where somebody, for various reasons, has lost control of the name. And in nearly all cases, we can help them get it back and the industry, generally, is very cooperative. So, when names have gone to another registrar, we will maintain pretty good personal contact with each other, and we can usually get the name back for the customer or get the control back for the customer.

Michael: Great. Can you talk about the specific incident that happened with NYTimes.com?

Bruce: Yeah, that was a case where obviously they were targeting media companies deliberately to take control of their names. And I think what has happened in the past, if you go back a few years, that the typical method was a denial of service attack. So, you try and generate a lot of traffic, and then blast the websites. Media companies can actually defend themselves reasonably well against that because it is mostly static content. It is not people logging in and making changes. When there is mostly static content, you can duplicate that in many places around the Internet, so it is fairly easy to defend that against a denial of service attack. So, what the attackers have instead done is said, "Okay, if we can get control of their domain name, we can then point their whole website to another location." And again, the hackers will try and find different ways through our registrar system, and most registrars, again, have hardened their systems pretty strongly, so it is pretty hard to directly hack a registrar or somehow find a flaw in the software that they are running.

Michael: Right.

Bruce: But the weakest link is often a human link, and so what they have done is they have found by, I guess, searching on the Internet, looking at various sources, they have identified the names of employees of companies that are looking after a media website, and then they have constructed what is called a spearfishing email. The reason why it is called spearfishing is because it is very targeting. It is not like a scam where you trying to confuse somebody into handing over millions of dollars or whatever. Some of the scams, but they are broad-brushed. They are sent to millions of people. A spearfishing email is saying, "We do not know exactly, but it is one of these ten or twenty people that are probably involved in managing this domain name. We will send an email to them that looks like it is from someone they know." It could be from a colleague. It could be from their boss. It is an email that looks like the sort of email that you should open. And the email is constructed in a way that, one, it looks like it is from someone that you know and trust, and the subject looks like something you should investigate. And then inside the email is a link, and you are encouraged to click on that link, and then you get some sort of message that comes up and says, "Oh, look, whoops. Your access to the system seems to have dropped. You better reenter your username and password." And because you think you are in a trusted environment, you have opened an email from someone you trust, you have been sent somewhere that says, to proceed to the next step, you need to reenter your username and password, and it is done in a way that you think you are perfectly safe and you do that. Then the hackers have actually got a username and password, which they can then use to access the domain name account where the targeted domain name was located.

Michael: Right. And is that what happened with the New York Times? Did the Syrian Electronic Army send a bunch of targeted emails to people that they thought might be in control of the domain name registrar account?

Bruce: Yes.

Michael: And one of those people signed into a reseller from Melbourne IT?

Bruce: Yes, that is correct.

Michael: And once they had access, that is just like me signing into my registrar account at GoDaddy. I can change any of the information that is in there without any oversight.

Bruce: That is correct, yes.

Michael: All right. A lot of times I will get an email from a registrar, saying, "Some information on your account was changed." Do you know if all registrars do something like that, where they confirm via email any changes to an account?

Bruce: Yeah, that is certainly available. In these situations, often it is a reseller account, and it is slightly different account to a normal consumer account, because it is assumed that if that would be happening, they would be getting lots of emails all day. And so, generally, that kind of feature is not turned on.

Michael: Ah, I got you.

Bruce: And then that reseller, in turn, is managing the customer, and it depends on, again, what the customer wants from that reseller.

Michael: Right. And so, when they sign into a reseller account, so they did not go into MelboureIT.com.au. They went to some third party account that actually connects into your system. They sell domain names and hosting on behalf of Melbourne IT. Is that correct?

Bruce: Yeah, that is right. Yeah. In this particular case, they would know that they have come to Melbourne IT, but they would also know that they are accessing a reseller account within Melbourne IT.

Michael: Got you.

Bruce: So, yeah, basically have the name of the reseller, but it would also be clear that it is Melbourne IT.

Michael: Okay, I understand. And then they basically change information in the reseller account, and then that computer connects to your computer and updates in your computer, and then it propagates around the web. So, what they did was they changed where that domain name - NYTimes.com - points to; and instead of pointing to the New York Times web server or system of servers, they pointed it to some other place where they actually were trying to install spyware on the computers that visited.

Bruce: Yeah. As far as we know, there was no attempt to install spyware or anything on computers. A lot of these more politically motivated attacks typically are not malicious in the sense that they are trying to harm users. What they are really trying to do, typically, is, most commonly, embarrass the target company and then get some sort of political message out. So, rarely, in those cases, do we see malware or spyware; and in this case, we have no evidence of that.

Michael: And they want to target large companies with broad bases like the New York Times. If they targeted DomainSherpa, for example, they would only reach a very small portion of people and they want to get their message out as broadly as possible.

Bruce: That is right.

Michael: So, that is why companies like the New York Times or large multinational companies that would be featured in the news for a hacking incident are more targeted than small companies like mine.

Bruce: That is right. Yeah, and increasingly, they are targeting Government websites as well. Same concept. If you are unhappy with a particular Government stance, you try and access one of their high-profile websites and say, "Look, this Government is wrong and this is why."

Michael: Yeah. So, once the New York Times noticed that their website was not pointing at their web server and it was pointing to a different location, how long does it usually take in order to fix something like that so that it correctly points to the proper location?

Bruce: Yeah. Actually, the actual fix is almost instantaneous. And one of the things that was interesting in this case is I would see hours, even a day later, people saying that they could not reach the relevant website. And the reason for that is the Internet protocols are designed to be fairly resilient in that your computer typically remembers where it has recently been, and so it does not have to keep asking for the translation between the domain name and the target location where the content is. So, typically, you will keep the information for about 48 hours. And so, what happens in these cases is: let's say a domain name changed in the next five minutes. So, in five minute's time, the domain name is going to change. Now, if I visited the website right this instant, I am actually going to have the right answer, if you like, for the next 48 hours. So, I actually will not even notice the attack. It will not even hit me, because I have already stored the correct information. But then I have some downtime for five minutes, so I put some bad information in there for five minutes. If a user happens to visit your website during that five-minute period, they will store a copy of that wrong information and then keep it for 48 hours. Someone that then logs in ten minutes later, after I have fixed it, will actually pull the correct information.

Michael: Right.

Bruce: So, it is one of these funny things. Because there was Twitter feeds and various things going out, saying, "Hey look, this website has been hacked," a lot of the people in the community go: "Oh, I better go and have a look," and mostly journalists. And so, in doing that, all the journalists within this period of time stored the bad information, and then, when they kept going back, they kept saying, "Still down. It is still down." It was not actually, and for most users it would not be, because the average user did not look at it ten minutes ago and is looking at the new information and they have got the right information. Someone that looked at it yesterday has still got the right information from yesterday and will not be impacted either. So, you get this strange impact where people are screaming, "It is down, it is down," but probably only for ten percent of the users. Just ten percent of those users who are in the media industry.

Michael: Yeah. And when you say your computer is storing the wrong information, it is not actually caching and strong the content that is on the webpage. It actually storing the location - the IP address - of where that domain name should point it, which web server it should go to.

Bruce: Yeah, I am simplifying it a little bit.

Michael: Right.

Bruce: Typically an Internet service provider will actually store some of that information in their network, and therefore the impact can impact the members.

Michael: Ah, so there is multiple places. It can be my computer. It can be my ISP, like Comcast, that stores that domain name server (DNS) information for the domain name. So there could be multiple ways that this issue is being confounded.

Bruce: That is right. So, once the sort of, if you like, the root cause, which was the change of the domain name. That was fixed very quickly, but then I think the issue was then contacting ISPs and others and saying, "Flush/Reset your computers," so that they get rid of that bad information.

Michael: So, they need to flush out the DNS records that they are storing. Is that what it is?

Bruce: Yeah, that is right. Yeah.

Michael: Okay. And do I have to do that on my local computer? Like if I run a company. Let's say I just upgraded my web service, and it was pointed at one website and then I moved it to different server, a different hosting company, and I pointed it to the information that that new host gave me. But I am still seeing the old website on my computer. Is there a way that I can flush that out of my computer or my ISP?

Bruce: You certainly can do it at the computer level, but it is beyond what normal users would be able to do. I mean mostly, when you are doing a deliberate change, you just have to assume it is going to take 48 hours to take effect. That is a common number you hear in the industry.

Michael: 48 hours.

Bruce: So, you plan it and normally, if you are going to do a DNS change, you do it on a weekend or something so that your customers are not effected, or in the middle of the night or whatever.

Michael: Yeah.

Bruce: But typically a change takes what we say is 48 hours to propagate, which means within a 48-hour period all the computers around that network have reset themselves. Some straightaway, but 99% within 48 hours.

Michael: All right, great rule of thumb to keep in mind for anybody that is updating their website and pointing their DNS at a different server. So let's talk about how people and businesses can prevent their domain names from being stolen or hijacked. What are some different ways that they should make sure that they are aware of, Bruce?

Bruce: Yeah, I think there is probably three things. The first thing is take advantage of auto renew to at least make sure your name does not accidentally expire. The second one is what is referred to as a registrar lock, which is essentially a lock on your domain name within your service provider. And what that lock does is it stops the name being transferred to another registrar. And that was a method of hijack that was common about ten years ago, where you would front up, or a malicious party would front up, to another registrar and they would say, "We are moving our business to you. Here is our domain name." And that would setup a whole series of automated steps, but it was actually possible to transfer the domain name to another registrar and then change the records. So, now, mostly registrars automatically put a name on lock when you register the name, and then if you want to actually transfer it to another party, you log into the registrar and essentially turn the lock off, and you also get a special password called an Authorization Code that you have to give to the new registrar. So, a couple of factors of authentication there essentially that you have to turn a lock off, you have to get a special transfer passcode, and that has reduced the incidents of being able to hijack by moving it to another party first.

Michael: Right.

Bruce: But essentially, the protection is to make sure your name is locked at the registrar. And then the third method of protection is commonly used by larger companies, which is referred to a registry lock, and that is a lock at the core database that stores the DNS information for the domain names. And what that actually does is it turns off all the automated processes. And so, to make any change on the name requires manual; essentially staff to staff contact. So, a staff person at a registrar is actually directly, manually, contacting a staff person at the registry and exchanging a security code to make that change happen. So that means it is going to be slow. So, if you were an end user, you would have to contact your registrar. Probably ring them up. They would have to work out who you were, so they would have a process for identifying who you were. Once they have identified who you were, then they, in turn, contact the registry and the registry has a whole series of checks to verify that they are talking to the right person at the registrar. And then the change gets made. So, really, you would have to plan it a day ahead. You could not just make a change when you wanted to. And if you got it wrong, you would have to go through the whole thing again, because it is not going to get switched back again either. Same protocol, so you have got to make sure you plan it carefully, you make the change and you get it right, because there is no going back. It will take you another 24 hours to get through that process.

Michael: Yeah, that seems pretty laborious to go through that process. Do a lot of companies take advantage of a registry lock like that?

Bruce: I think there is two aspects of it. I think one is there is a lack of market knowledge that this lock exists, and typically it is a case of closing the door after the horse is bolted. And often you will see companies that have got their name on registry lock have probably experienced some issue; and in response to that issue, the registrar said, "You can put it on registry lock," and they go: "Great, we will put it on registry lock." But often, at the time when their names are coming up for registration or renewal and the registrar mentions it and says, "Look, I have got this extra feature. It will add sort of 24 hours of time. It costs more because we are doing manual processes," a lot of them just say, "Oh, no, we will not worry about that. We will be fine."

Michael: Right, because they do not even understand why it is of benefit to them

Bruce: That is correct. So, I think we certainly recommend companies, because a lot of large companies are running big IT departments and they do not make changes very often. And when they do, they have got a whole IT team that does testing and checking and so on. So, we recommend it for large companies, but mostly for what we call their primary domain name. So, if it was a company like, say, IBM, then obviously IBM.com is their primary name; you would want to protect that. But they might have other names. They might have Mainframe.com or Storage.com, or something. And if something goes wrong, it is not the end of the world, but for their main, core domain name, you probably want every protection you can get.

Michael: Right, and that was actually the case with the latest Syrian Hacker episode. One of the domain names of Twitter was on registry lock. Not the .CO.UK, but the .COM, I believe, was on registry lock, so the attackers could not change the domain name server records - where the domain name actually points.

Bruce: Yes.

Michael: But they did change the WhoIS information - what actually displays as the registrant of the domain name when people look it up.

Bruce: That is correct. Yeah, so pretty much, as far as the end user was concerned, they saw no impact with Twitter, because their name was on lock. The other thing to understand though is that that registry lock is not available for all domain name types.

Michael: Oh, okay.

Bruce: So, it is available for .COM and .NET. It is available for .COM.AU in Australia, but it is not yet available for .CO.UK. That is an example (Unclear 24:51.6).

Michael: Okay, I understand. So, back to the second way to protect your domain names. It is the registrar lock. I think, by default, aren't most domain names that are registered today locked by the registry by default?

Bruce: Yeah, that is right. Most registrars do that by default and you explicitly turn it off. It varies, but certainly you would want to make sure that, at the very least, your name is on lock, and you can usually log into your registrar account and verify that, because like other sorts of locks, sometimes the registrar will make you take the lock off to make certain changes. And so, somebody could have taken the lock off for some reason, but forgot to put it back on, and things like that.

Michael: Right. Now, it seems like the big security hole to the registrar lock is that if you get access to the email account on record for that registrar account, you pretty much have full access to do whatever you want to the domain names in that account.

Bruce: That is right. If you manage to get access to somebody's email address, then you can then go to not just registrars, but any really online service, because most online services, whenever you click 'forgot my password', it basically sends new credentials to that email address. So, definitely protecting the credentials for your email is very important. And I think the other thing that is probably increasingly recommended these days is to have more than username and password control on your email account. Have some other factor. It might be a text message gets sent to your mobile phone and you have to enter in a code, or sorts of things that are becoming more prevalent in the online banking industry. If you have got a million dollars in your account, you probably do not want to just have a username and password to access it.

Michael: Right, exactly. Two-factor authentication. And with the new iPhones coming out, talking about putting a thumbprint on that, that might be another factor authentication in the future. So, if you want to transfer out or do something really significant to a domain name - change where it points, transfer it to another registrar -, maybe you have to use that factor to authenticate.

Bruce: Yeah, I think that is right. I mean we are sort of investigating some additional factors that we will provide, and that has varied over time. I like the thumbprint idea. That kind of depends on having it widely available in devices. So, if the iPhone has that feature, that would be great. Going back a few years ago, you would typically get some sort of electronic token. And that is great if you were doing something every day, but like with a domain name account, you probably only touch it once a year. People would then lose the token, so you are forever sending tokens out. And then people go: "Oh, I want to make a change." You go: "Well, where is your token?" They go: "Lost it," and so we will mail it to you, but that will take a day or so. And so, that is the tradeoff, whereas the fact that most people have a mobile device means that some use of the mobile phone in authentication is helpful. But even then, people leave their phones in taxis, and a lot of the times the phones are not properly protected.

Michael: Right.

Bruce: And probably that is one of the weakest security links today; is that there is lots of software that you can put on your PC. You have got passwords and encryption, and all sorts of things, whereas a lot of people will store all their passwords on their phones, and then they will lose their phone in the taxi. And so, I have got their password on the phone and I have got their phone. You can do a lot of damage with that.

Michael: Definitely. Well, just having access to their email right then. They can sign on to Amazon. It will probably remember them. They can make a purchase. They can sign into the registrar and request an email password change. It comes directly to the phone. They can check it. So, yeah, there is a lot of different ways that hackers can gain access to your email account, which then controls so many things.

Bruce: So many things, yeah.

Michael: Do you recommend that people not use free email accounts or only use a specific email address for domain name administration, or anything like that, Bruce?

Bruce: Yeah, I think one of the challenges actually is that we have a system of basically publishing the details of the person that is registering the domain name, and the system is called WhoIS. And the problem with that is it actually opens you up for social engineering attacks, because you know the person's name and address, which you can use in other forums. So, you actually ring someone up. And they might say, "Okay, I just want to verify who you are. What is your address?" Well, you have it because it was published on the WhoIS, or you can actually target their email account because that email account has been published. And so, I think, yeah, if you want to be really particular about your security, perhaps use a different email address that is published in your WhoIS from your email address that you might use for private communications.

Michael: What about WhoIS Privacy? There is a way to obfuscate all of the information that somebody can use to look up. So, if I go to WhoIS.DomainTools.com and I look up DomainSherpa.com, it will tell me the registrant information, which is actually my information, but do you recommend that I pay extra money to my registrar to hide all of that information and then have information sent through a third-party service to me?

Bruce: Yeah, we certainly offer that service to users. I think about 30% of people typically take up that service at the time of registration, but that is probably increasing. I think we are probably seeing it now getting closer to 50% at the time of domain name renewals, presumably because they think: "Well, my name is actually getting more important now and I do not want to really have this information published." So, increasingly people are selecting that option. I would certainly recommend it if you are using your home address for a domain name. A lot of small businesses operate from home. Often it is a second job. They have got a day job and then they are operating a startup business from home, and they use their home address to register the domain name. So, in that case, I would certainly recommend taking advantage of the privacy service. Another thing is, when you are dealing with more corporate uses, it might be best to use a role name rather than your actual name. So, you might say contact name is Chief Technology Officer at Melbourne IT rather than Bruce Tonkin, for example.

Michael: And are you allowed to do that by registry rules to not use a real person's name as the registrant, but to use Domain Administrator or Chief Technology Officer, or something like that?

Bruce: Yeah. The actual name of the domain name in that instance, the organization name is the legal name of the company that is applying. So, the actual registrant name, if it was our company, would be Melbourne IT, so that is the actual owner of the name. And then the role-based contacts are often better because people change in roles and so often companies will use roles like Domain Administrator or IT Manager, or things like that. And often that is more useful because you can ring up a company and say, "Can I speak to the IT Manager?" And if the person changes, that is fine. And bear in mind that a lot of corporate names are registered for ten years, so there is a reasonable chance that the person that registered the name is not there in ten year's time.

Michael: Right. Are there services that will monitor your domain name for any changes and email you if anything does change?

Bruce: Yeah, there is. Yeah, there are quite a few services that you can employ to monitor changes in DNS records. It is subject to the sorts of issues I mentioned earlier. That okay, you get a notification that your records changed. Yes, you can change it back. That is easy. The trouble is the fact that people have stored the old/bad information for a period, so the impact lasts for longer than the few minutes it takes you to fix it.

Michael: Right, but if I somehow lose access to my registrar account, I can use a third party tool to monitor my domain name and tell me if it is actually pointing at a different location.

Bruce: Absolutely, yes.

Michael: And does Melbourne IT, as a registrar, offer a service like that?

Bruce: Yeah, we used to. We actually sold. We had a more corporate focused division, which we have sold in March of this year, but something (Unclear 33:49.6) we will have another look at because a lot of the services that we are offering purely to corporates we only provided through that division, including the registry lock actually. And then, with this most recent incident, we realized that a lot of smaller businesses have been contacting us, so we are starting to launch a lot more or make available a lot of the services that we have provided to big companies to small companies as well.

Michael: Great.

Bruce: Yeah, we will certainly look at that.

Michael: And I will just throw out that I do know of at least one service that does that - DomainTools.com, where you can sign up for an account and they will monitor a certain number of domains for you and notify you if there are any changes. So, if you want a third party just watching, that is an opportunity as well. So, we talked about a lot of different ways for people to protect their assets - their domain names - so that people do not get access to steal the domain name from them. The worst case of stealing, of course, is then they get access to the registrar account, they unlock it at the registrar, and they request the EPP code - the authorization code - that allows them to transfer it to another domain name registrar. What can happen if a thief does do that, Bruce?

Bruce: That is always very problematic because it has gone away from your current supplier, and the new supplier could be in China. It could be in a completely different country, and so then you do not have the access to the local laws presumably, so you definitely want to avoid that. Having said that though, the first point of contact would be to go back to your original registrar, because that registrar has probably got the best chance of contacting, through their own private channels, the other registrar. And there is a fair bit of cooperation in the industry when those things happens, which is fairly unusual, but when it does, we tend to cooperate with each other to get the name back to the rightful owner.

Michael: So, if I have a domain name stole, somehow they get the domain name out of my account and into another account, and I can determine that by doing a WhoIS lookup of the domain name at any of the registrars, including Melbourne IT or WhoIS.DomainTools.com, and look it up and I see that it is in another registrar. What you are saying is that it is to my advantage to contact my old registrar - my current service provider - because they are more apt to be able to get information quicker by directly dealing with the new registrar to resolve the issue.

Bruce: That is right, because otherwise you call up the new registrar. You will be talking to their customer service. They have got real no knowledge of you. They do not have any credentials to verify who you are, whereas if you are dealing with your original registrar, they can validate who you are and validate that it is genuine, and also that it is not just forgetting to renew the name situation.

Michael: Right.

Bruce: Because most commonly when I hear that - another register or another person has got my name -, most common it is because they have failed to renew the name. And realistically, there is not much you can do at that point other than rely on the good will of the new owner. And sometimes the new owner might go: "Oh yeah, you can have it back," but if they choose not to, there is not much you can do.

Michael: Right. And if I have a domain name registered at Melbourne IT, do you have records of all the transactions that happen on my domain names so you can see that I registered on this date, I have renewed it a certain number of times, I signed in on this date, I requested an EEP code and then transferred it out?

Bruce: Yes. In fact, all registrars need to keep records. I think it is for about seven years. So, yeah, part of our registrar accreditation is accurate record keeping and we do have those records.

Michael: Great. So, the first thing that someone should do if they notice their domain name is stolen, whether it actually is stolen or it is just not resolving to the location that they think, is to contact the support group at their current registrar?

Bruce: Yes.

Michael: Okay. All right, I think there is a lot of great information here, Bruce, that definitely clarifies the situation. Final question for you. Let's say that I have a domain portfolio for my business. It is a hundred different domain names, some of which are high-value, either because it is attached to my business or maybe just investment for domain names. Let's say that I have done all the things that you have suggested. I have got a secure password. I have got two-factor authentication on my email. I have really secure passwords on the registrar. Maybe I am using privacy on the registrar so you cannot even see that I own it. If I pass away and I tell my wife that I have got this portfolio, how does she get access to the list of domain names? And let's assume that I am a good husband. I am not hiding anything. I want her to have the portfolio. What is the process that she would go through if I am doing all the right security precautions that she can get access to the account?

Bruce: Yeah, it is actually a very good question because the other problem that (Unclear 39:11.5), and it happens at a couple of levels. We often actually get caught up in disputes. It could be divorce. It could be a business relationship between two people. You are working together and you are getting along great, and one person says, "I will just register the domain name." You go: "Fine," but they register it in their own personal name.

Michael: Great point, yeah.

Bruce: Yeah, the business relationship fails or the marriage fails, or whatever, and then you go: "Well, I would like to access that name." It is like: "Well, you cannot, because it is not in your name." I think it is really not much different to how you would treat a house or a bank account in that certainly it is important to actually make sure that if it is a company that you actually register it in the name of the company, not the employee, because that is a common mistake, because if there is dispute at some point, all we have is the name of the person that registered the name. So, you want to make sure you use proper company name. And then the other scenario is obviously if you are registering it for personal reasons and it is a family situation, you would want to make sure that is properly documented. And I guess your scenario of a death in the family, that is treated like any other asset, so, in your will, you would say, "My wife or whatever should have access to this asset, and these are the details behind that asset." As long as you have got documentation, then you can take that to the registrar and say, "Look, my husband was John Smith, and he has now died. Here is his death certificate. Here are the legal papers that now mean I am the rightful owner of the name," and then the registrar will transfer the ownership of that name to the relevant partner.

Michael: Okay, and my wife, in this case, would just go to the support group, or open a support ticket, or call the support line to initiate this?

Bruce: Yeah, usually what happens: I do not know exactly how all registrars operate, but certainly Melbourne IT has a sort of general customer service area, but we also have a more of a complaints area that is managed by sort of paralegals who, in turn, report to lawyers. So, typically, any dispute of that nature would go actually through to our legal team, and I know GoDaddy and other big registrars do the same, and they will just look for appropriate documentation.

Michael: Excellent, and so great advice for a business partnership. If two principles have split up; if one of them has the domain names in his or her name, that could be problematic. Put it in the company name so that it is treated as an asset just like all the other assets of the company.

Bruce: Absolutely, yes.

Michael: Great. Great idea. All right, if you have additional questions, please post them in the comments below and we will ask Bruce to come back and answer as many of them as he can.

Dr. Bruce Tonkin, Chief Technology Officer at Melbourne IT. Thanks for coming on the Domain Sherpa Show, sharing your knowledge of security, and thanks for being a Domain Sherpa.

Bruce: Thank you.

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

Watch the full video at:
http://www.domainsherpa.com/bruce-tonkin-melbourneit-interview/