

SLIDE 1: (VIDEO START TO 0:00 TO 1:10) Welcome to Digital Footprint 101: What Every Business Owner Needs to Know Before Something Breaks. This is what I'm going to refer to as kind of a, I'm going to try to make this as non-techy, but it is still somewhat technical of a tech talk, because these are items about your digital footprint, about the things that, um, your business's online presence, that you need to know. We're going to talk about things like logins, things like where things are registered as far as your domain goes, who's your host, all of those things. So we're going to talk through those key components of what makes up your digital footprint, what they are, why they matter, and what you should know in order to stay in control of this. Because losing control of any part of your digital footprint can be really catastrophic for your business. And I've got a few examples that we'll give along the way here, um, but hopefully you're going to leave with clarity on what pieces make up your digital presence, control over who has access to the platforms, or at least you'll leave with a plan of how you can get control of those, and then the confidence to manage or delegate those access controls without panicking. So that's what our goals are for today.

SLIDE 2: WHAT IS DIGITAL FOOTPRINT? (1:10 – 2:26) When we talk about your digital footprint, as far as your business goes, we're talking about everything about your business that exists online. This usually starts off with your domain name that's your web address, your www.yourbusiness.com that's your domain name. Then you've got your website. If you use domain-based email, you've also got your email address. Even if you use Gmail or, um, you know, if you have a Hotmail account or an Outlook account that you're using um, any email, any email that you're using for your business. We're going to talk about that a little bit. And social media directories, so the listing of your business in a directory, review websites, things like Yelp those types of things and then any other digital tools. So that might be email marketing, it might be any other CRMs, or any type of database you're using. Those all make up your digital footprint. We're not really specifically going to talk today about directories or review sites. If you want to know more about that, we do have a webinar about what we would consider reputation management and getting control of your directories and review sites, so you might want to go check out that webinar as well. We're really going to focus mostly on those first four bullet points your domain, your website, your email address, and your social media.

SLIDE 3: DOMAIN NAME, YOUR DIGITAL ADDRESS (2:28 – 9:24) First, talk about your domain name. This is your digital address. Your website actually exists on an IP address that's a numerical-based IP. So, you probably have seen it like 65.149.67.2. Technically, your website exists at that IP address, but you have a domain name because a domain name is much easier for people to remember. It's much easier for me to say, "Hey, just go to ProFusionWebSolutions.com." You could remember that and go to my website, rather than me giving you some numerical-based, um, you know, IP address that's really hard to remember. So, the domain name is that memory-friendly way that people can access your website. You do not own your domain name technically, you're renting it from a domain registrar. Now, a registrar is someone like GoDaddy. It could be Namecheap or Google. Google even had a domain service for a while, but they've since sold it to Squarespace. So, you may have had Google as your domain provider, and now you have Squarespace Domains. If you don't know where your domain is registered or when it expires, finding this information out is your priority number one today.

On my screen, you'll see I have up the domain information for my company, ProFusionWebSolutions.com. You'll see it shows the date it was registered, and I have highlighted the date it expires. So, on January 29th of this coming year—2026—if we do not go in and renew our domain name, if we don't go to our registrar and renew it, it will expire, and someone else could then go purchase my domain name. A competitor could buy it, someone else with the same company name could buy it, or just someone else could go up and purchase it. If that happens and it has happened. We've had a few customers who, when we're not in charge of the domain name, have let their domain expire or lapse in registration. Then someone else buys it, and trying to get that back is expensive or not possible at all if the other company is going to use it.

Now, it might seem really silly you might be thinking, "Well, of course you're going to register your domain name; of course you're going to renew it." But the problem is, you can register your domain name for one year, or you can register it for 10 years. People who are registering it for 10 years if you think about 10 years ago, what was your email address? Did you maybe have an old AOL email address that you were using that you no longer have access to? Well, it's possible that if you registered your domain name 10 years ago, you used that old AOL email address, and now all of your renewal notifications are going to that email address that you no longer check.

So, when you're renewing or registering a domain name, think about how long you want to renew it for. Maybe two or three years might be a good period, where you know you've got the domain name secured and you know that you're going to have

access to the email address you're using to register that domain name, to be able to go in and renew it. Now, you can set your domain name to be on auto-renew with most registrars. So, in GoDaddy, for example, you can set the auto-renew, and that does give you some peace of mind. However, just remember that credit cards do expire. Credit cards get hacked, or you might have canceled a credit card, and you might not have updated it in GoDaddy. So, just think through all of those things when you're registering your domain name. You want to register it for a good enough amount of time to where you feel comfortable that you've got the domain name, but not so far out that you might be creating a problem that you're not even aware of yet. You might lose access to that email address, like I said. So, when you're registering that domain name, again, just get it for a good amount of time and make sure that your contact information remains updated. You obviously can go into your registrar and update your contact information should your email address change. It's just one of those things that people don't typically remember to do.

The expiration date there is one really important thing to look at. I've also highlighted on the screen the name servers. The name servers are actually telling me—as someone who understands the technical side of things—where this domain name is hosted. So, that ns.sourcedns.com—that doesn't mean much to anyone. That's not the web address you're going to go to, but looking at this, it tells me where this domain is hosted.

Further on in the presentation, you'll see I have a couple other screenshots where this information actually gives you some clues as to where your website might be hosted. You might see Squarespace in here. You might see Network Solutions in here, and that gives you an idea of where your domain is hosted—where that domain name server is hosted. Now, the registrar information is the other thing we have outlined in red there. It's a little grayed out because we didn't want to give away too much information here. But this would show the registrar where your domain name is registered. This could be GoDaddy. You might see Tucows. You might see Squarespace. Whatever the information is, it's going to tell you where you actually registered the domain name.

So, if you pull out anything from this presentation today, what I want you to do is go and take a look, and you can get all this information by going to Whois.com. If you go there and enter in your domain name, it's going to tell you when your domain name expires, what your name servers are, and where it's registered. That's the registrar information. Just go jot that down. At the end of this presentation, you'll have the opportunity to get a little checklist where you can write all this important information in there. And that would be if you do nothing else today go get this information and then make sure that you have access to that account, the registrar account. So, if it's a

GoDaddy account, make sure that you can go to GoDaddy, log in, and actually see that you have that domain name in your account.

Okay, so that is your domain name. You need to know who the registrar is, when it expires, and then take a look at where that DNS is pointed that's the name servers so that you can see who's actually hosting your domain name.

Now, I did also highlight the registrant contact there. Again, ours is grayed out on that, but you would see who the owner is. If you've opted for a private registration, this might show "privacy," "privacy redacted," something like that. But if it actually has a name there, just make sure that the name is the right person within your organization. That might be your name as the owner, or you might have a CTO—a Chief Technical Officer—that might be their name in there. It might be your web developer's name if you want them to be the person in contact about your domain name. Just make sure that the name that shows under the registrar contact is someone that you are familiar with and that you have communication with. Hopefully, it's you or the owner, or manager of the business. So, your domain name is typically your first and most important part of your digital footprint—that ownership of your domain name.

SLIDE 4: WHAT IS YOUR SITE BUILT WITH (9:24 – 14:10) Now, let's talk a little bit about your website. So when someone goes to your domain name, your website is what loads up at that point, uh, most websites right now are powered by what we would call a CMS, or a content management system. That would be something like WordPress or Wix, Squarespace, or maybe Shopify if you're running an online store. Those are some of the more popular ones. If you've ever logged into a dashboard and been able to update a blog post or add a page to your website, that is you logging into a content management system the thing your website engine that runs your website. So, when you have that, it's important to know what your website was built with. So, was it built using WordPress? Was it built on Wix? So, understanding and finding out what your content management system is, and then what tools or plugins were used to create your website.

If you're using Shopify as your content management system for your e-commerce site, for example, you might have a plugin that allows you to use Authorize.net as your payment gateway for credit card transactions. And that might cost you an extra \$35 a year. Now, if you don't renew that if that doesn't come up for renewal and you don't renew it then your credit card processing might go down on your website. So, if you don't know what tools have been used to actually create your website, and you don't know when those licenses renew, you could create a situation where your website

might not be working. And you might not find out until, you know, someone actually takes the time to pick up the phone or send you an email and say, "Hey, I'm unable to process a transaction on your website." So it's important to try and stay ahead of the game on that by making sure that you understand what tools have been used to create your site. And if they have renewal dates what that is, how much it costs to renew the plugin, and then what that license is. So, actually get that license code to be able to license that product. In order to do all of that, you obviously need to know how to access the back end of your website. I've got some tools here that I'll show you in just a second.

But there are a couple of different ways that, if you really don't know what your site was built with, we might be able to help you with that. And then the last thing I just want to address is making sure you know who has access to your website. I can't tell you, after again 20 years in this industry, how many times I've logged into somebody's website only to look at their list of users and see that they have, you know, past employees that still have access to their website. Or they have old developers that still have access to their website. The more access points you have into your website, the higher the chance of either it getting hacked because there's different usernames and passwords out... There that you don't know, or if you have someone who, you know, just messes around with your site, there's more opportunity for things to go wrong. Anyone who's an admin on your site they're able to edit content, they can also add and remove users, so it's possible they could remove you. They can change the settings, and they could even take the site offline. So, all things we are hoping to avoid. Now, if you really don't know what your website is—how, what it was, what it was built with—there's a couple different things you can do. The first one is, there's a web address on my screen right now, and it is just whatwpthemeisthat.com. And if you go there, if your website is a WordPress website, and you copy and paste your web address into the box you'll see on that screen, that's going to tell you if your site is a WordPress website. For the most part, if your website uses is built in WordPress and uses some tools that hide some of the WordPress characteristics, it may not be able to detect it. But for the most part, it's going to be able to tell you if your website is a WordPress website.

Alternately, you can also go to your domainname.com and add—again, I'll make the second bullet point here on my screen—addwen... Admin to your domain name, and if that pulls up a login screen, then that tells you that your website was built with WordPress. That's what the "WP" stands for WordPress admin. That's just a standard WordPress install. If there haven't been any security plugins used to hide that login screen, that's how you can tell that it's built with WordPress. And then the other thing you can do is check your DNS settings. So, like I showed you on the first screen when

we were talking about domain names, check your DNS settings to see where your name servers are pointed. I took a screenshot of one of our a client that we're working with who's working on using Squarespace as her website provider. And this is her DNS settings, so you can see where it says Squarespace DNS in there, and that just shows that her website is built with Squarespace and is currently using Squarespace as the host. Talking more about DNS again. You can see the name servers there. When I have the name servers pulled up, that shows you all the DNS settings there.

SLIDE 5: DOMAIN NAME SYSTEM (14:11 – 21:57) And if we look at your DNS, it's really like the traffic controller or the phone book for your domain name. It helps translate your domain name—like ProFusion Web Solutions—into the technical instructions needed to connect your website, your email, and any other services that you have on your domain name. This is, again, probably as technical as we're going to get, because this is not something you're going to log in and deal with on a daily basis. This is typically—you're going to set this one time and then not ever touch it again, unless you're changing where your website is hosted or changing where your email is hosted. Those are two times you might go in and change these settings. And typically, it's not the business owner who's changing these. If you have a technical person on your team, they're typically the ones that are going to go in and make these updates. Now, just to show you that—and again, there's an action item related to this one too—but this is typically what your DNS zone records are going to look like. You're going to have—you see that left column on the screen there where it shows you the type? You're going to have multiple types of records. You see there's an A record, there's a CNAME record, there's an MX record, there are those NS records—those are the DNS records we've been talking about—and then there are some text records, the TXT records. Now, what each one of these records has is kind of a different job. The A record is telling people where to go to find—it's not telling people—it's telling the browsers, the actual browser like Chrome or Edge or Firefox, where to physically go when someone types in that web address.

If I type in ProFusion Web Solutions, that is the IP address under that data column there. That's the IP address where that website actually lives. So that's the physical address for—or the actual address of—where it lives on the server. The CNAME record that you see there is email verification. This actually tells me—if I look at this, if this was a potential client's—this would tell me that this client hosts with Outlook. So they have a Microsoft account that is typically—uh—is hosting their email. Uh, then it shows me the CNAME record for DKIM, and then—and we'll talk a little bit about what DKIM is here in a second—uh, it gives me a CNAME record for the Uh... What we call a canonical URL—to make sure that if someone types in www.domainname.com or

domainname.com, that it goes to the same place as if someone was not using the "www." So it gives you the opportunity to set where that actually goes with the "www." And then you see the MX records. That stands for Mail Exchange. That tells you uh, the email records. So that is uh —if someone is sending you an email—this is how, really quickly behind the scenes, your email goes and says, "Hey, I just sent an email to Patrice@websolutions.com. Where should that actually go?" And this is the record that goes to the domain name. It tells that email that was just sent to me how to be delivered to my inbox. And then we have the two NS records. Again, those are the DNS records—those are the main traffic controller that kind of controls all of this. And then we have a text record for SPF and a text record for DMARC. Now, quickly—I don't need you guys to remember any of these acronyms or any of what this means—just the gist of: there are things that are important to your domain name, and these are a few of them. Specifically, the A record is for your website. So that's going to tell people—or tell the internet—where to find your website. And then you specifically want to make sure that you have your MX records set up if you're having domain-based email, because that's going to be sending people through, you know, Gmail servers to get to your Google Suite, or Outlook to get to your inbox. So, A record, MX record—almost every business that we work with has these. Where we see people go a little bit wrong on their domain name—on their DNS records—is with the SPF, the DKIM, and the DMARC. The SPF helps verify which servers are allowed to send email from your domain name, and that stops spammers from being able to pretend that they are you. So I couldn't just, you know, set up an account and start sending from a domain name that's not mine. If a user had—or a domain—had the SPF record, it specifies who can send email on behalf of this domain name. The DKIM adds a digital signature to your emails, proving that they come from you and haven't been tampered with. These are all behind the scenes, right? So you set this once time on your domain name, and then every time you send an email, it's doing this work behind the scenes. It's nothing that you're going to have to do on your end every time that you're sending an email. And then the last one that we see most people don't have set up correctly is the DMARC. This tells receiving servers what to do if an email fails those first two—the SPF or the DKIM checks. They either flag it, quarantine it, or reject it completely.

So those three things—SPF, DKIM, and DMARC—are three things that we typically see maybe are not set up at all or not set up correctly. And that's one big thing—if your email is not being delivered, if people say, "I, I, I found your email—it was in my spam folder"—if you're hearing that a lot, it's possible that those three culprits are what's wrong on your DNS record. So the action steps for you is to go to whois.com. You're going to enter in your domain name, find out who your registrar is and who your host is—your DNS host—who's hosting this record, this zone record that we're looking at on

my screen right now. From that person or company—let's say it's GoDaddy, let's say it's, you know, Network Solutions, or it could be a company like ProFusion Web Solutions—we might be your host. Request a DNS zone record export from your DNS host. Just keep this for your records. It'll look like what you see on my screen right now. So you're going to be able to see an A record, you're going to see if you have CNAME records set up, you're going to see whatever is on my screen there.

You're going to see what all of those records are that are set up for your domain name. You don't need to do anything with this necessarily—just a good idea to have an idea of what your records are. So you know the IP address for your website, you know that your email's hosted with Outlook—it's going to give you a little bit of those clues to unlocking all of the mysteries of your domain name. So again, having this report is going to tell you where your email's hosted if you have those MX records set up. It's going to show you if you have the SPF records set up, and the DKIM and DMARC. And it's going to give you a backup should you need to restore any of this data. Okay, I'm going to jump real quick and see if there's any questions, because I know that was a super heavy—uh—kind of tech, a tech-heavy slide there. So let me just take a look and see if there's any questions. And—none yet. So I've either pushed you all to sleep, or that was clear as mud.

Hopefully it's one of those—or hopefully it's neither of those.

Okay, so that's—that is DNS. Again, I don't need you to remember the acronyms. All I really want you to know is—you have a record of where all of these things are hosted and what all this information kind of means from a high level. We don't need you to, you know, memorize any of this data. But just from a high level, understand that these records make up anything—when someone is accessing your domain name, they're being told to go somewhere, right? So if I go to your domain name, I'm redirected to that IP address. Even though it doesn't show the IP address, that's in the A record, right? So it just gives you information on your domain name and where all the services are hosted.

SLIDE 6: WHO HOSTS YOUR DOMAIN-BASED EMAIL (21:57 – 25:50)

All right, so let's take a look more specifically about email. For most businesses, if email goes down, that's the first thing. You know—usually then you start to see that error in Outlook, or you see that your, you know, your outbox has a bunch of emails that haven't been sent yet. And that is a really big indicator that there is something wrong with your domain name. The first thing to know is—your email might not be hosted in

the same place that your website is hosted. So, if your website host is GoDaddy, you may not host your email with GoDaddy. You may have your email at Microsoft or with Gmail. We have a lot of customers who host their website with us, but have their email provided by Gmail or Microsoft, or an alternate email provider. If you're a doctor, you might use a more HIPAA-compliant email provider. I know there's a lot of security settings involved in that. So those your host, your website host, and your email host—might not be the same person. The one way to be able to find out is: where do you go to log in to manage your email? So if you go to—if you're a Microsoft user and you have, you know, Microsoft 365—you probably have had to go through the authentication situation where you're authenticating your email with Microsoft's authenticator. If you're using Gmail and you need to add an email account to your suite, you're going and you're logging into the Google Suite. You're not logging into Microsoft at that point. So typically, there's going to be some clues as to where your email is hosted. If you have domain-based email—if you're logging in at [mail.yourdomainname.com](mailto:yourdomainname.com)—that's a good indicator that you might host email in the same location that you host your website. Okay, so just little clues there as to where it is actually hosted.

What you want to do with your domain-based email is you want to make sure you know your login credentials. So, if you're the administrator on the account, you want to know how to log in to make sure that you can manage any accounts that exist on your domain name. Again, one thing we do when we're doing kind of an audit or cleaning up someone's digital presence is going through and taking a look to see what email accounts exist on your domain name. If you have five employees, but you've had some turnover and you have old email accounts that still exist on your email account, going in and clean those up to make sure that there aren't email addresses that are not active on your account.

First of all, it's probably going to save you some money. And second of all, it just again makes it so that that email address can't be used to send. You know—if that email password is weak or it's been part of a data breach—you want to make sure that you're closing as many of those holes as you possibly can. So, making sure that there are no email addresses out there that are just not being used, that are no longer active. So, going in...And cleaning those up. And then again, just making sure that if you are the business owner, that you are an administrator on that email account so that you can log in, you can see if there is an alias account being created, you can see if your employees are taking up a ton of storage on your email—maybe see what's going on there and clean that up a little bit.

But just being able to have access to the admin portal so that you can manage all of that information that's in your email, and being able to make sure that you're managing the accounts that are in your inbox, is going to be very helpful if anything does go down on your email. Now again, knowing who hosts it is going to help you be able to make sure that you know who to call in the event of something going wrong. So, if the G Suite—if you're using Google Suite as your email host—and let's say your email goes down, then calling your website provider isn't going to help, right? So your website provider is not Google, so they're not going to help you with your email necessarily. So if your email goes down and you're using Gmail, you're going to want to make sure that you have all of the Google contacts for the Gmail support on that.

SLIDE 7: GOOGLE BUSINESS PROFILE (25:50 – 27:55) And speaking of Google, we're going to talk quickly about Google Business Profile, just because this is becoming more and more critical. I know I said we weren't going to really touch on review sites at the beginning of this, but I do want to Uh quickly touch on Google Business Profile, just because this one is a major indicator in getting your website found—especially in local search—or getting your business found, especially in local search. So, uh, what I would encourage you to do—your action step on this one—is to go to business.google.com and log in. And when you do that, you're going to see a screen that's very similar to what is showing up on my screen right now on the right-hand side there. And it's going to show your business on Google, and it shows I'm currently the manager for the ProFusion Web Solutions account. And if you were to click on these little three dots here and click on "Business profile settings," what this is going to show me is who has access to my Google Business Profile.

Once again, this is something where we see a lot of business owners give access to past employees or old agencies that they've hired, or, you know, their cousin who said he could help them out but then has since, you know, decided to move on and be a firefighter. You know, there's all kinds of people that have access to your Google Business Profile. We've seen this happen, and that is a dangerous situation for such a critical component for your online presence. So go in there and take a look at your business profile settings. And again, it's going to show users and managers at this point. And take off anyone who doesn't need to be there. Make sure you keep yourself on there—obviously it's not going to let you remove yourself if you're the main owner—but maybe keep yourself and then one other trusted business adviser on there to make sure that you have one or two people on there. But if you have old employees, old managers on there, you do want to clean that up. This is important because they can

change any of your contact information on the internet. They can change or read, and respond to reviews. They can upload pictures. They can change posts. They can answer questions that have been asked. So if you have someone on there who maybe doesn't have your best interest at heart for your business, that is not uh, you want to make sure that just gets cleaned up. We don't want people who shouldn't have access, having access to our Google Business Profile.

SLIDE 8: EMAIL MARKETING TOOLS (27:56 – 30:47) And the same thing goes for email marketing tools. So, uh, whether you use Mailchimp, Constant Contact, ActiveCampaign—there's, you know, a hundred other platforms that you could use for email marketing—but these tools are more than just a way to send newsletters. They can also be used to—they often house our entire contact list: clients, leads, prospects. That list is incredibly valuable.

Our list is one of our most valuable assets as a business. So the question here is: do you know who can log in and send emails from that account? Again, there's often times where you're, you know, maybe trying to go through the setup process and you've given access to somebody else. You want to just make sure that when you look at your user list, that all of those people should be on that user list. I've had...A client who currently has lost access to her email marketing because she, first of all, didn't have her email address updated. She signed into email marketing with a—uh—an old employee email address, and then she deleted that email address and now no longer has access to receive her two-factor authentication. So now she's going through the process of exporting everything, trying to get everything set up again, and trying to reconfigure all of her segments that she had in that list and all of the contacts. So she's lost all of her data, her history, and no longer has access to her old campaigns either. So again, just a word of caution, who has access and how are you logging in? Make sure that you're logging in with your identity and not with an identity that somebody else set up for you.

And then the other thing I want to just kind of bring attention to here is—how is data being added to your email marketing tools? So if you have a form on your website that's a newsletter signup form, and if someone fills that out, they automatically get added to your email marketing list—that is great. But you're going to want to make sure that you have a double opt-in set up, or else you're adding a bunch of junky, potentially spammy email addresses to your newsletter, and you're maybe potentially paying for those as well. Again, so if you have just a newsletter signup button on your

website and you're not having a double opt-in, there's going to be all kinds of spammers who are going and just adding their email address to your site or to your newsletter. And really, they're just—they're filling out the form. That's what these spammers do. So they're filling out that form, but that email address is being added to your Mailchimp or to your Constant Contact. And if you're paying by number of people that you have subscribed to your list, this can make it so that you're paying too much, because those email addresses aren't any good. They're not actual contacts. So if you have an automated feed happening, make sure that you're cleaning that list occasionally, or make sure that you have that double opt-in added so that when someone does sign up, it sends them an email and they get the opportunity to say, "Yes, I really do want to receive email from Patrice or whomever." And then—and then—the person gets added. So make sure that you have that double opt-in added on email marketing tools.

SLIDE 9: SOCIAL MEDIA ACCESS (30:50 – 34:40) All right, let's talk about social media access. Again, I feel like we're a little bit redundant on what we're saying here, but just making sure that you're going through and you have access to all of your social media accounts. So the first thing we're telling you to do on your action items is—go through and make a list of all your social media handles. So we are @ProFusionWebSolutions on almost every platform. So Blue Sky, uh, Twitter, and Facebook, and Instagram, and LinkedIn. On almost every account, our handle is the exact same. The handle is your actual identity on those platforms—ProFusion Web Solutions. And then log in to each one of those accounts and see who can manage them. Facebook and Instagram use the Meta Business Manager, and within that platform, really specific items that you can give access to. So you can choose to provide access to someone for just having access to be able to post. You can provide access to someone to be able to manage your files. You can provide access to someone to just manage your ad account on Meta. So go in there. But again, you're going to see that there are potentially people who were helping you at one point in time with your social media accounts that are still listed in those pages as administrators that need to be cleaned up. I will say Facebook is the most problematic social media account that we deal with, where we're dealing with business owners who didn't set up their own social media accounts. They had somebody else set it up for them. Either—we've heard intern, we've heard cousin, we've heard their child has set up these accounts. But what that means is they don't have direct administrator access to the accounts, and they're going through a secondary party—they're going through another person to get access to it. And I cannot caution you enough as to why you

want to make sure that you have access to it. Uh, they're implementing the authenticator to make sure that you actually put in an authenticator code or you have some other data point besides just your password to be able to log in.

And it's unlikely that you're going to be able to continue to log in using somebody else's credentials. So make sure that your Facebook and Meta specifically is tied to you—the business owner—to your Facebook account. Um, if you don't have a Facebook account for you personally, go create one for yourself. You don't have to do anything on it. Just make sure that it's tied to your person and your email address, and that way, you can do your authentication on that account. Again, we've seen Facebook accounts that have 20,000, 30,000, 40,000 followers that were set up, that are active, and that have been now restricted because the owner doesn't have access to them.

They were accessing it through an employee. When the employee leaves, they get locked out of their account. And Meta is not an easy company to deal with when you're trying to get access to your account. We've gone so far as having to—um—we've uploaded the owner's ID, we've uploaded the owner's and the business license, and the articles of incorporation showing that they are the owner.

And Meta has still denied access to the page because they weren't the original owner who set it up. So, just make sure, before you get into any of those issues where you have to claim ownership, that you, as the business owner, are listed as the owner on each of those accounts. Transition ownership or admin rights to a business email or to your email that you control, if you do not already have it. Okay, again—and that's across all of them. So if you're on—even if you've just claimed your business name on Twitter but you've never logged in, maybe you don't even tweet, it's not something you're even into—you might need that one day. So make sure that it is tied to your email address and not to somebody else's.

SLIDE 10: EMERGENCIES HAPPEN – BE READY (34:41 – 36:10)

Emergencies happen. They do. I can't tell you how often a domain name has been reset. So that DNS record—that was the traffic controller for all your online presence uh, we've had times where a client has gone in and renewed their domain name, and when they renewed it, it wiped clean that zone record. So it took out all their records just by renewing it. They didn't check the little box that said, "Keep my zone record where it is right now." It updated it, and then everything goes down—website down,

email down, not able to send emails because of it. So, make sure that when you have that happen, something will go wrong. And the fastest way to recovery is knowing who to call or where to log in and figuring out what services are affected by that outage.

So, having that list—again, we have a checklist that I'll send out to all participants. You can also request it on our website on the webinars page for this. When we get the archive up, they'll have a registration form there that you can get the checklist. That's going to show you exactly what to put in—so who your registrar is, who your DNS host is, who your email provider is, and then a place for you to jot down—maybe if you have a company that is helping you with that—who they are and the phone number of where to call them. So, who to call, where to log in, and what services are affected are going to be—if you have that information when an emergency happens, that's going to help you get on the fastest path to recovery.

SLIDE 11: QUESTION & DISCUSSION (GET IN TOUCH) (36:11 – 39:21)

Let me jump in and see if there are any questions here. Uh, yeah, good question. So, a question just came in: "If I don't have access or I don't know any of this information, can you help me find it?"

We absolutely can. So we can help run an audit on your domain name and try and get you access, specifically to the domain name, to all of your email, and your domain name and all that. Having us help you get access to your Facebook page or Instagram account if you've lost access—again, that's a struggle. And it can be done. I don't want to say it can't be done, but it can be a challenge to reclaim ownership if you've already lost it. Uh, if you're just simply looking to make sure that you are the owner, we can help you through that process as well.

That's a good question. But yeah—or if you just don't have a starting point, you don't know where to start—start with the checklist. Download that checklist from our website, and that's a good starting point because we'll at least give you the web addresses as to where to go, and just create that cheat sheet and then revisit it.

So on the checklist, you'll see that we recommend that you revisit that once a year. So when you go and renew your domain name, just do a quick check and make sure that maybe you haven't changed email providers, or maybe you've now moved from Mailchimp to Constant Contact. Just go through it and update all of those items so that you have, you know, a 2025 or 2026 domain review or digital footprint review, and you know exactly where all your digital assets are hosted and can be modified.

I know that was a boatload of information, and I tried to keep it as non-techy uh as possible. But DNS is—again—it's one of those things I can't tell you enough that every business owner should know this information about their digital footprint, so that they don't lose it. Because it's expensive. Not only in trying to recover it, but it's expensive if you've done SEO on your website and you've got great rankings, and maybe you have a Google Ads campaign that's driving traffic to your site, and then all of a sudden your domain is expired and someone else has purchased it.

It's really hard to recover from that. It's hard to then purchase a new domain name and set up a new site, and get your site back on that new domain name, and then start to get the rankings and recover from that. It's incredibly challenging and something that I don't wish upon any business owner to have to go through.

So having access to these things and knowing where the domain name is registered and when it expires—even again, if you get nothing else from this webinar but just those two things today—that is going to make sure that you're just ahead of the game so that you're not losing work that you've already put time and money into.

Have any other questions? All of our contact information is on the screen right there. If you want to contact me directly, just change that info at to patrice@profusionwebsolutions.com.

That's our main phone number on there. We do post very regularly on Instagram, on Facebook, and on LinkedIn with just helpful information like this. So feel free to head on over and give us a follow. And if you have any questions, please do reach out. We're happy to help at any time. Thanks so much, Reier!

