**WHAT YOU’RE DOING TO INVITE HACKERS & WHAT TO FIX FIRST**

**Chalene Johnson**: Previously on The Chalene Show.

Check your Twitter. I think you just got hacked.

My heart’s racing now because I realized that this person is sending tweets like mad. And it seems as though he’s got a ring of friends who are all in on this together. And at the same time, he starts taunting me in social media. “I hope you’re watching. I now have control of your over 400,000 Instagram followers.” But every account that I check, every account I try to log in to, I’m denied. I’m like, “Oh my god. Oh my god, oh my god, oh my god. No. No, shit. How can this be happening?”

All they need is to gather enough information about you and work diligently to crack the code on just one password. What city were you born? What high school did you attend? What’s your favorite movie? What’s your mother’s maiden name? Every application you’ve ever filled out is a public record. Leases, the cars you’ve purchased, schools you’ve attended, job applications, online services, everything. It’s all out there.

You must recognize that my story could be your story. I know this happened for a reason. I’m not going to let it defeat me. It’s got me riled up and ready to share with the world what we can do to protect ourselves.

**Male speaker:** Welcome to The Chalene Show.

**Chalene** **Johnson**: On Saturday, June 6, 2015, just days ago, my social media accounts were hacked. Since that time, my life has been turned inconveniently upside-down.

There’s much more I wish I could share with you. Unfortunately, or fortunately, depending upon how you look at it, because the FBI is involved and the United States Attorney General has agreed to take this case on, I’m not able to share additional details.

However, I know that this happened for a reason. I know I foolishly left myself exposed to the world. I thought I had no enemies. I couldn’t imagine why anyone would want to hack me. Well, my friends, it has nothing to do with notoriety, or enemies, or money, or anything else for that matter.

Every day, hundreds of thousands of Americans have their information exposed online. And not everyone has the kind of connections that get the FBI to stand up, take notice, and act quickly. In that regard, I got lucky.

This week, I’ve heard from hundreds of everyday citizens, business owners, moms, grandpas who’ve shared with me stories of having their identity stolen, cars bought in their names, social media sites hacked, you name it. And it’s difficult to track these people down.

It’s up to you, it’s up to me. Our information is out there. Your information is out there. If somebody, right now, wants to know your phone number, your home address, your mom’s maiden name, it’s all out there. If you own a cellphone, if you’ve ever filled out an application ever in your life, even your grandpa’s information, it’s all out there.

Can we ever protect ourselves 100%? Probably not. You know, if somebody wants to get in, they’re going to get in. But we can be much smarter about it.

Today’s guest knows a lot more about this than just about anyone else I know, that’s for sure. He’s a former DEA special agent with connections to the FBI and this is what he does. And helping people to protect themselves and to just be smart online is something he takes very seriously. He’s helped me through all this. It’s so hard to say. He’s helped me to gain an appreciation for this subculture, these people who do this. And to help me help thousands of people protect themselves.

Darren, first, a huge public thank you. I just - thank you isn’t enough. I just have to start this off by saying so much of this - I mean, because of your connections, legitimately, because you’re a former special agent, because of your knowledge, because of - honestly, you were kind enough to stay on the phone with me for hours and hours and hours and connect me to the right people. Because of those things, that’s the only reason why I’m actually able to record this podcast today.

For those of you who have been following this story, Darren is the individual who I referenced as this whole thing unfolded. In the mindset of, you know, 10,000 text messages that I was receiving while I was, you know, obviously under this public hacking, I got a text message from your wife. And she said, “Hey, we see that you’ve been attacked and Darren wants to help you. So call as soon as you can.”

I immediately jumped at that offer because you and I had spent some time talking about security and like things we should do and just a couple of weeks earlier. So I knew you had this knowledge, I knew this - your background and, you know, the connection you had with the FBI and the DEA.

I just have to say, the reason why people need to listen to this podcast, I’m in this like weird, very special, very lucky position, because when this happened to me, I reported it to the FBI and I could just sense that it was going to go in the pile of all the other cybercrimes.

And, Darren, it was when I reached out to you and you were able to, you know, get the other agents on the line and connect that story to all the right agents who had the right connections and I know - we can’t disclose too much, right? But that’s the situation most people aren’t in. And I got really, really lucky and it is because of that. I have to say thank you and we can help educate people today.

**Darren:** It’s my pleasure. And I have to commend you on handling this the way you did. A lot of people would be in absolute disarray. When you picked up the phone and you weren’t just falling hysterically, I was like, “Wow, she has this together.” I think we’re going to make some traction.

**Chalene Johnson:** Yeah, that came later. I think it was - I knew, because of your connections, I was in the right hands. Even though I knew I needed to just be patient and I was kicking myself for not doing these things earlier.

But I want people to recognize that even with my notoriety, it just - it didn’t help. It didn’t matter to anybody until, you know - luckily, you’ve been working with individuals that you were able to make those right - like, literally, connecting me on the phone to the right departments. And the FBI getting really almost excited about, you know, the information we were able to give to them that I just - I really think this happened so that, number one, I had to learn from it and number two, that people have to understand this can happen to you. And it has nothing - well, you know what, if we can, can I just hit you with some fast, rapid fire questions?

**Darren:** Absolutely. Let’s do it.

**Chalene Johnson:** Okay. So, how many people do you - maybe you know the answers to this, but how many people in the United States have this kind of thing or they’re information exposed each year?

**Darren:** Well, it’s estimated that in 2014 alone, about 47%...

**Chalene Johnson:** 47%?

**Darren:** …of American adults had their personal information exposed by hackers.

**Chalene Johnson:** Okay. I’m going to follow-up with that. Do they know they’ve been hacked?

**Darren:** Not necessarily.

**Chalene Johnson:** Or they’ve just been exposed?

**Darren:** Many don’t.

**Chalene Johnson:** Okay.

**Darren:** And literally, all it takes is one click on an infected advertising banner to get a full access now to your computer.

**Chalene Johnson:** Mm-hmm. Okay. Facebook. Are we safe on Facebook especially if we’ve got a really creative password? Can you get hacked on Facebook?

**Darren:** Absolutely. You’re not - just never assume that you are totally safe.

**Chalene Johnson:** How common is that?

**Darren:** Every day. Every day.

**Chalene Johnson:** Wow.

**Darren:** 600, 000 compromised logins a day. Think about that for a second. There’s 800 million users on Facebook and every day, 600,000 of them are compromised. That’s one login every 140 milliseconds. Just put that into perspective for a second.

**Chalene Johnson:** Like so many people don’t even consider how important it is for them to use Facebook for their business.

**Darren:** It’s what they count on.

**Chalene Johnson:** Yeah. Okay. So then, if I have a scrambled password, am I safe?

**Darren:** No.

**Chalene Johnson:** Okay. If I turn off my computer at night or if I think someone’s compromised my computer – if I turn off my computer, am I safe?

**Darren:** No.

**Chalene Johnson:** Okay. Do they need, like, information on me like my Social Security number or my date of birth in order to hack me?

**Darren:** No. It helps.

**Chalene Johnson:** Okay. Can I assume, if I am not famous or, you know, I’m a nobody, am I safe? Like why would anyone want to hack me?

**Darren:** Because it’s easy.

**Chalene Johnson:** Okay. Good point. It seems like most - I can only speak for myself. I knew I needed to do the things I’ve since done. I just kept thinking, “Well, I mean, I don’t have any enemies out there and it’s kind of inconvenient and I’ll get to it when I get to it but I assumed it would be super inconvenient.” Is it inconvenient?

**Darren:** No. And it’s a minor, minor temporary inconvenience compared to, say, recovering from a hack like you’re going through now.

**Chalene Johnson:** Oh, my gosh. I can’t even, I can’t even, I can’t even. Okay. Is it expensive to put in the types of security and, you know, levels of protection that we’re going to talk about today?

**Darren:** Absolutely not.

**Chalene Johnson:** Do I need to be a techno guru?

**Darren:** Yes. You have to be a genius. You can’t do anything if you’re not - no. No, not at all.

**Chalene Johnson:** Okay. And, okay, lastly, if you’re just a nobody, right, like you’re just - I don’t mean that to sound the wrong way, but like you’re like, “I don’t have fans. I’m not even on social media and, you know, I don’t put myself out there,” are there places - if you think you’re incognito, are there places where people can just buy your personal data?

**Darren:** You can count on it. There are lots of places out there where people can obtain your information.

**Chalene Johnson:** Can I clean that off the Internet, completely?

**Darren:** There are companies that offer those services. Again, be very careful on who you trust online.

**Chalene Johnson:** Mm-hmm. Yeah. Okay, interesting. All right, well then, let’s get to this. I promised people and I didn’t want to leave anyone hanging and I want them to know there’s a lot to do, clearly, right? And you can never be 100% foolproof. That’s for sure, I’ve learned that.

But I want to take people who are like, “Okay, you’ve got my attention.” I get it and I want to use this medium to help educate. And I want to walk people through the process because so many people reached out to me and they’re like, “Where do I start? What do I start with?”

So let’s take people back to day one and we take them through a checklist, basically of, “Okay, what’s first?” What is first? I realize, “Okay, I’ve got to take security more seriously.”

**Darren:** Right.

**Chalene Johnson:** What’s the first thing I need to do?

**Darren:** Well, before you even embark on step one, you need to really appreciate why you need to do it.

**Chalene Johnson:** Okay.

**Darren:** So, kind of how I like to equate the necessity for security is this. Think of your existence as a vault of knowledge and skill that you contributed to and invested in your entire lifetime.

**Chalene Johnson:** Mm-hmm.

**Darren:** Therefore, the net worth of you is literally invaluable. And just like banks protect themselves from thieves, you have to secure you.

**Chalene Johnson:** Mm-hmm.

**Darren:** Criminals are going to inherently choose the easiest route of access. It’s all about getting in and out as fast as possible. And the easier you make it for them, the more open you are to a quick attack.

**Chalene Johnson:** Yeah.

**Darren:** Right? So you got to also appreciate the level of person you’re dealing with. A lot of people like to hate on these people for what they’re doing. But in reality, these guys are artists. And I got to say, they are bad asses. I respect what they do because there are a lot of very intelligent people out there. So you have to respect their ability.

We like to hate on them for the damage they caused because it’s inconvenient for us. But remember, they are masters of their craft just as we aspire to be in our own respective fields. But, we also don’t have to make it simple for them to take advantage of our neglect.

**Chalene Johnson:** Hard for me to admit that but you’re right. I mean, you’re right.

**Darren:** Don’t make it easy for them. And honestly, they’re going to appreciate you at least making an effort, like that one who reached out to you.

**Chalene Johnson:** Yes.

**Darren:** You know?

**Chalene Johnson:** Oh, I’m like, dude - you know, once one of them was communicating with me, I’m like, “I’m fascinated, and I’m annoyed, and I’m really angry right now but I’m also fascinated by what you do and how this -“ like you said, it’s like, where else can they connect as a community and get this thrill? And I wanted to know the mindset of it and how do they learn this.

And it is very interesting but the one thing he said right away was that it’s, you know, it’s fun. They call it LOLs or, you know, they’re like, “It’s a good time.” You’ve helped me to really calm down about this and understand it from their perspective and to give them the respect that is due.

And I can still be mad and I don’t have to agree with what they do. But that did help to calm me down and understand the perspective of it, like this is their craft.

**Darren:** Mm-hmm.

**Chalene Johnson:** And it might be illegal, but they’re not all bad guys.

**Darren:** Right. And, you know, like, like I said before, some of them end up with jobs at the very companies they penetrate because they’re helping them now patch those holes and release those updates.

**Chalene Johnson:** Yeah.

**Darren:** So I mean, if you think about it, I mean, if you can throw a baseball 100 miles per hour, you’re probably going to find a way to get paid to do that.

**Chalene Johnson:** Mm-hmm.

**Darren:** And they’re just doing that with what they can do.

**Chalene Johnson:** Okay. Got it. Let’s move.

**Darren:** All right.

**Chalene Johnson:** What do people need to do first?

**Darren:** Well, number one thing, and this is probably my biggest pet peeve that I see all the time whenever I’m with someone and I see their computer, or their phone, or tablet, whatever it might be. And you see that little badge and it says 27 updates.

**Chalene Johnson:** Oh, yeah.

**Darren:** Oh, my gosh. Number one thing you can do, update your software. Update your software. And when possible, go ahead and enroll for automatic updates. So whether that’s on your computer, or most importantly, something like Adobe Flash which tends to have a lot of holes and a lot of people to get in that way. So, update Adobe Flash. Go and turn those automatic updates on.

And that is huge. It’s huge right there. Remember what I said? They can gain access just by clicking on that banner. So if you click on that banner, you might’ve just let somebody in.

**Chalene Johnson:** And I think it’s important that you say that first because as we were starting to, like, go through absolutely every device that we’ve ever owned, in most cases I had to say, “Okay, now we have to update.” Because we hadn’t updated software in a couple of the devices we have in our house and so we had to do that first. I’m glad you said that number one.

And number two is to share with people that I would see those updates and, you know, you think, “Oh, I never use this computer. I’m not going to update it.” Or, “It’s going to take too much time.” So you’re saying…

**Darren:** Right.

**Chalene Johnson:** …every time you see that, these companies that are providing the update, they’re not going to say, “Hey, there’s a breach of security. There’s a hole.”

**Darren:** Yeah.

**Chalene Johnson:** “There’s a bug.” They’re going to say, “There’s an update available.” But what we should be aware is when we see an update, that means there’s a possible risk for security.

**Darren:** Yes. Here’s a fun little thing to try. When you’re in the app store and you see that update, click on show more and look at the actual change log. See what is actually being patched here. See what the fixes are. A lot of time you’ll see bug fixes, right? How many times? Facebook, for example, they release updates every week and it says that in their thing. So, every week they release updates and its bug fixes, right? Bug fixes, but what are those bugs?

**Chalene Johnson:** Okay.

**Darren:** You know, what are those bugs?

**Chalene Johnson:** Okay.

**Darren:** So, you got to think about that. They’re not just releasing updates because it’s fun. You know, sometimes there are new features but when you see bug fixes, they are fixing things that were found in potential vulnerabilities that can let people in.

**Chalene Johnson:** Okay. That makes sense. All right. So now I’m going to start updating. Everyone is going to start doing that in a regular basis.

**Darren:** Yes.

**Chalene Johnson:** And were going to auto update if possible. Now, what do I do?

**Darren:** Next, number two, most important thing, get a password manager. Get a password manager. Now, my favorite one is 1Password. There are other alternatives. People like LastPass. I just happen to be a big fan of 1Password. Many of the people I trust in the tech community all love 1Password as well.

It’s available across devices, across platforms. And it’s very, very good software. And then, it’s easy, intuitive and it’s usable for everyone, everyone.

**Chalene Johnson:** Can I just say tell you the only thing that I don’t like about it?

**Darren:** What?

**Chalene Johnson:** The name.

**Darren:** 1Password?

**Chalene Johnson:** Yeah, because when you’re trying to - like, you know, I was trying to explain to - because I’m like, “Okay, so, you’re going to get a password, your 1Password.” And like I keep saying - like, they’re like, “Wait, what’s a 1Password?” I’m like, “Well, that’s the name of the software.” So, I - we started nicknaming it 1P in my house just…

**Darren:** 1P**,** yeah.

**Chalene Johnson:** …like we were explaining it because often times you’re explaining it and talking about passwords so it got confusing.

**Darren:** Well, if you think about the name, though, it originates because form this point forward, you really have one password, a challenging, but memorable enough to type often password that’s going to secure your vault.

Now, people are often concerned, well what if somebody gets access to my vault? Aren’t they going to get all my passwords and all my information and credit cards and social security numbers and everything that is stored in there?

Well, your master password isn’t actually stored in your vault where an attacker could get it. It’s actually not stored anywhere at all. So, if you forget it, tough luck, you can’t get into your vault.

That’s the reason we can’t recover it. There’s no security questions with this one. So, you want to choose one that you remember. And what I recommend doing is in your spouse or relative or friend or whoever, have them put your master password inside their vault.

**Chalene Johnson:** You can write it down and put in in couple different places in your house. I mean what we’re…

**Darren:** You can.

**Chalene Johnson:** ...trying to do is protect ourselves from online attacks, right? So, it’s okay to have it written down a couple of places in your house, am I right?

**Darren:** Until somebody breaks in, finds that piece of paper…

**Chalene Johnson:** They won’t know what I mean…

**Darren:** …logs on your computer…

**Chalene Johnson:** I swear.

**Darren:** …gets there.

**Chalene Johnson:** So, in other words, don’t put it on your computer.

**Darren:** Yeah, just, if you’re going to write it down somewhere…

**Chalene Johnson:**  Put it in a book.

**Darren:** Just don’t have it on a sticky note…

**Chalene Johnson:**  Not front.

**Darren: …**on the front of your computer, please.

**Chalene Johnson:** Got it. Yes. Okay. Dad, did you hear that?

**Darren:** It’s surprising how many people do that.

**Chalene Johnson:** Now, let me tell you this. I had a different password manager on my phone. And I had been using it to store my passwords I was making up. So, I want to clarify that for people. This is not - well, it can be but the best way to use this is not just a place to simply store the passwords you’ve made up. Tell us how this works.

**Darren:** All right. So, think of 1Password as the wallet that you would keep in your purse or your pants. That wallet is going to have all your important digital information. So, it could have your passwords, it could have your driver’s license, it can have your credit cards, it can have your identities, addresses, secured notes, those things that people love to just write down and keep it in a tucked drawer, if it has sensitive information, write a secure note inside 1Passwod. This is all protected by and encrypted by your master password.

And, what I said before by it being a cross-platform, what I love about 1Passwod is that you have it on your Mac or PC. And you also have it on say your Android or your iPhone.

Great part about the iPhone is using what’s called Touch ID, that finger print. I’m so surprised how many people refuse to set that up because they think it’s an inconvenience.

**Chalene Johnson:** Oh, I love it.

**Darren:** But in reality, it’s amazing.

**Chalene Johnson:** Yes.

**Darren:** So, instead of having to type that long master password, you just have to use your thumb print to unlock that vault if you enable that feature in the settings on your phone. That’s a very nice time saver so to speak from having to type that master password every time.

**Chalene Johnson:** It’s beautiful.

**Darren:** You still have to type that, when you turn your phone off and back on or after 24 hours of inactivity. But, as much as you use your phone, that Touch ID is going to save you.

**Chalene Johnson:** Okay. So, I download this app or buy the software if I’m on my desktop computer.

**Darren:** Yes.

**Chalene Johnson:** I open it up and, you know, I notice tutorials for each one of these but generally speaking most of them you can either type in your password or am I correct in saying that most of the top ones anyways will create for you an encrypted long impossible for anyone to remember password.

**Darren:** So, yes, you’re correct in that it creates a unique password.

**Chalene Johnson:** Okay.

**Darren:** And that’s what we recommend doing. For every account that you use, create a unique password for each account. So, instead of using your dog’s name backwards and a number, use a unique password. And you can come up with that yourself, right? But that’s complicated, that’s tough. You got to write that all out.

So, you use 1Password or your password manager of choice to generate that random password. What’s nice about this is is you can then define the length. You can define whether it should use digits, symbols. You can say the quantity of each.

And so what I recommend is when you are setting up your passwords, say if you’re in, I don’t know, Wells Fargo or something. And they tell you the length that you can have and they give you the recipe for what your password can contain. Follow that recipe and whatever the maximum is, do the maximum.

So, it says your password can be 8 to 21 characters, do you want to do 8, when you can do 21?

**Chalene Johnson:** Right.

**Darren:** No. Make it harder.

**Chalene Johnson:** Yeah.

**Darren:** Make it harder for them. So, that…

**Chalene Johnson:** And what’s so cool - and I assume this is the technology behind it like you don’t have to enter the recipe like you’re on that website, 1Password reads that field and says, “Oh, we can tell what it needs in terms of letters, numbers, symbols, et cetera and length.” And it does it in like two seconds.

**Darren:** It’s a nice feature. You referred to the browser extensions in 1Password…

**Chalene Johnson:** Okay.

**Darren:** Available for Chromes, Safari, Firefox. Please don’t be using Internet Explorer, but if you are…

**Chalene Johnson:** Okay.

**Darren:** …let’s focus on the other ones. Now, you can use that password generator to do that right from the browser itself. So, you can still define the recipe, you know, the length. You can define digits, symbols and it will automatically plug that in. Then it will save that login for you. I recommend titling it, going back to the app and titling it something that you actually remember because they don’t likely put wellsfargo.com. Name it like Wells Fargo personal or whatever.

**Chalene Johnson:** Like for example for me I’ve got multiple Instagram accounts.

**Darren:** Right.

**Chalene Johnson:** So, when I open up 1Password now, there’s all my Instagram accounts. And then, it doesn’t just say Instagram. It’s says the title of each account and then when I click on it, that’s where I can see all of my information.

**Darren:** And I glad you brought up Instagram because that’s one that illustrates exactly why this is such as nice thing to have. So, they don’t allow a fast way to switch between accounts, it’s super frustrating. Instagram, if you’re listening, please change that.

**Chalene Johnson:** Right.

**Darren:** So, what you do is you just go to the 1Password app. You click the copy button, you go back to Instagram, you paste it in. Very simple. You can set 1Password to now forget what’s copied on your clipboard after a certain amount of time. So say two minutes. That way it’s not staying on there all day. So, when you’re out there surfing on the web or on your accounts and you hit paste again, it’s going to past that again. It’s going to forget it after a set amount of time. I recommend doing that.

**Chalene Johnson:** Okay.

**Darren:** So, one of the beauties of 1Password is it allows you to create those automated generated passwords across all accounts.

So, don’t login to Facebook on every site that you use. You see that option a lot, right?

**Chalene Johnson:** Yeah.

**Darren:** Don’t do that.

**Chalene Johnson:** It seems convenient.

**Darren:** Because - it is convenient. It makes it super easy, but by that same token, it also opens you up should say your Facebook, you know, gets penetrated.

**Chalene Johnson:** Right.

**Darren:** So, then they now have access to all these other areas of your life.

**Chalene Johnson:** That’s right.

**Darren:** So, always, always set up a fresh account to everything that you use.

**Chalene Johnson:** Okay. So, when I’m like shopping online and it goes, “Hey, you know, login as a new user or would you like to use your Facebook account?” Say, no and open up your…

**Darren:** Say no.

**Chalene Johnson:** …account - okay got it. Having said that, most people have already done this. Shouldn’t they go back into their Facebook accounts and detach those apps from there…

**Darren:** They should.

**Chalene Johnson:** Okay.

**Darren:** And you can go into Facebook and you can see exactly where you were logged into and what apps are you’ve authenticated to use. So, you can go ahead and deactivate all those. Recommend probably, immediately after this, going and changing your Facebook information.

And this is going to segue us into the next couple sections of actually using two-factor authentication, one that’s called the code generator…

**Chalene Johnson:** Okay.

**Darren:** …to protect yourself further.

**Chalene Johnson:** Okay. That sound like - right there is where I think a lot of people put fingers in their ears and they’re like two-factor authentic - I can’t even pronounce it, what does this mean? Can you just explain it to us in layman’s terms?

**Darren:** Yes. So, two-factor authentication. Before we jump into that, I want you to understand the precursor which was what? Security questions.

**Chalene Johnson:** Okay.

**Darren:** So, initially we had security questions which everybody answers honestly. So, what street did you grow up? You answer it honestly.

**Chalene Johnson:** Yeah. So, you can remember it.

**Darren:** Exactly. So, what that does is that opens you up to whoever has that information answering your security questions honestly and gaining access to your account. This is where social engineering really comes in. And they take that information that’s available out there and they use it.

**Chalene Johnson:** Well, can we back up? In case someone didn’t listen to the last episode.

**Darren:** Okay.

**Chalene Johnson:** Which they need to, haller. But, what is a social - because I think most people assume that, you know, that hackers we’re talking about are sitting in a dark room, you know, cracking codes on computers. But this is a new type of, I guess you could say profession?

**Darren:** Right.

**Chalene Johnson:** What is a social engineer?

**Darren:** So, social engineering really is an art. It really is an art in which hackers use a psychological manipulation of people into performing actions or divulging confidential information. So, where do they get this from? Well, they can get it from you. You could divulge this information to them. Somebody could call up your house, say, “Hey, this is AT&T. Your account has been compromised. You need to identify the street you live on and your date of birth.” And they just got this information out.

Asking your security question, just right there. So, this information is available. Now, where else might they get this? Well, how many times do you know people who have been in the mall and they see that shiny cars sitting at the middle of the ball. And you can fill out that form to enter to win it. Everybody wants to win that so we fill it out, right?

**Chalene Johnson:** Right.

**Darren:** Well, by doing that, your information has now been sold out there. I’m not saying it’s being sold directly to hackers. What I’m saying is that information is going to be distributed to various sources which could then potentially get hacked.

**Chalene Johnson:** I think a lot of people assume like, “Oh, I’m very careful.” But if you filled out your name and address in a few other…

**Darren:** Right.

**Chalene Johnson:** …pieces of information, you’re everywhere.

**Darren:** You’re everywhere. It’s a new era. And if you think about just, just recently when Target was hacked, as many as a 110 million customers had their data breached.

**Chalene Johnson:** Oh my gosh.

**Darren:** 110 million customers. So this is happening and your information is going to in people’s hands. So, don’t just get reclusive and crawling to a ball and just say, “I can’t do it and I’m going to go back to a Zack Morris telephone and just send snail mail.” Just, chill out.

Realize all we can do is our best. These guys are brilliant at what they do. And that’s just the fact. So, you have to just make it a little bit more difficult, so that they’re hopefully going to move on to that person who wasn’t listening to the podcast. No offense to that person, but they should have tuned in.

**Chalene Johnson:** Right. Right, exactly. Okay, so then do all sites have the ability to have this two-factor sign-in?

**Darren:** No. They don’t, unfortunately. Instagram is a great example, right? So, if you want to know a great site to find that out is called Two Factor Auth, like authentication, just…

**Chalene Johnson:** Okay.

**Darren:** …abbreviated.

**Chalene Johnson:** Okay.

**Darren:** twofactorauth.org. It will be on the show notes and it will tell you the type of two-factor and whether or not it’s offered. So is it in SMS or is it an actual token that’s generated? So, what I’m referring to there is this. Two-factor authentication is basically you enter your password. And then, a code is generated and either sent to a mobile phone, say, for example or sent to a code generator, such as Google Authenticator or the one built into 1Password. Now, this might sound confusing so let’s break it down.

**Chalene Johnson:** Okay.

**Darren:** Single-factor authentication is just your PIN or your password. Single-factor, PIN or password.

Two-factor authentication is single factor plus a software or hardware-generated token or it could be a card or something like that. Now, two-step, you hear that often, two-step authentication is single factor plus a code sent to the user. So, say like text it to your phone.

**Chalene Johnson:** Okay.

**Darren:** Now, the one area and there was a case in which it was rumored that this was defeated. And somebody was able to get to a Gmail account set-up with two-factor because they were able to spoof the number. And they forwarded that the number to theirs, therefore receiving the code and then get in it. So, really protect yourself by answering those security questions dishonestly. I recommend generating random passwords for them, instead of just answering them dishonestly.

And that way they’re recorded and logged and you just copy/paste them should you ever need that. That way, somebody can’t go into, say, your Verizon or AT&T account and switch that information, right?

They can’t just take that and answer those questions and now they’re in, they’re forwarding your phone and you’re screwed. So, protect yourself with two-factor by using a code whenever possible. Facebook offers this. Dropbox offers this. Evernote offers this. All the major cloud services are moving in this direction.

**Chalene Johnson:** Okay. So, if there isn’t two-factor authentication on Instagram, what’s the worst thing that could happen?

**Darren:** The worst thing that could happen…

**Chalene Johnson:** How they going to get in?

**Darren:** …is you got hacked, what happened to you.

**Chalene Johnson:** Right.

**Darren:** So, what you do is you got to use that secure password. You got to made it tough to get into. So, generate a long random secure password whatever the amount, the length is allowed, generate that, use that. And then, answer your security questions dishonestly with a randomized password. That’s the best advice that I can give. Beyond that, I mean, all we can do is our best.

**Chalene Johnson:** Right.

**Darren:** Remember, all we can do is our best. So, if somebody doesn’t offer two-factor, then you just have to really think about what are my security questions and what is the email address that I am using to receive these password resets, right? So when you see that little ‘Forgot Password?’ link, somebody clicks on it, have you ever received one of those out of the blue, just, “Oh, you forgot your password?”

**Chalene Johnson:** Yes.

**Darren:** Yeah. Guess what? Somebody is trying to find out your password. We’ve all received those.

**Chalene Johnson:** Yeah.

**Darren:** So, that email arrives that you think to think about, is your email secure? Because if they can get into your email, as in your case, set up without two-factor, honest security questions, that type of stuff where they get access in, now, they can reset your password on everything.

**Chalene Johnson:** Yeah.

**Darren:** Right? So make sure that the email address that you are using on file with any of these services is protected with two-factor. Gmail is a good one. Google, obviously. If you don’t have two-factor, generate a very secure password.

**Chalene Johnson:** Well, I know we were going to talk about phones, and we’re almost out of time, but we have so much more to talk about, right?

**Darren:** Yeah.

**Chalene Johnson:** I mean, like what you’ve shared with me thus far, how safe is the average person if they listened to this, they’re like, “Okay, I took notes and I’m going to do these four steps. I’m going to start with this,” how safe are they?

**Darren:** You’ve taken a baby step. We’ll put it that way.

**Chalene Johnson:** Okay. But this is a minimum, right?

**Darren:** There’s much more…

**Chalene Johnson:** Like now you know better.

**Darren:** This is bare minimum.

**Chalene Johnson:** Okay.

**Darren:** Bare minimum. It really is. And you get - we’re going to get into email, phones, how to protect yourself across all these different platforms.

**Chalene Johnson:** So we can continue?

**Darren:** We can continue or we can come back to it another day, however you’d like to proceed.

**Chalene Johnson:** Okay. I’m going to have to do this the way I would personally know I would implement. And that’s how I try to treat my lifers because they’re just like me. And now I know they’re taking this far more seriously. And if we overwhelm people with like 85,000 steps, it just feels like, “I’ll take my risks,” right?

**Darren:** Right.

**Chalene Johnson:** So I want people to just follow through on those things that we went over today and start there. And, Darren, can I have you back?

**Darren:** Absolutely. We’ll continue in a part two.

**Chalene Johnson:** Okay. Let’s do a part two. I can’t promise people it’s going to be tomorrow, but as quickly as possible. I know nothing is safe, but what are the safest, what are the ones that are the easiest to compromise - emails. And then what are we doing on our phones that’s compromising our security.

And then I think we also need to talk about, you know, just our kids and what they’re doing with their phones and how we share accounts. And let’s get into that in our next episode, if we can. Are you down with that?

**Darren:** Absolutely. We have much more to discuss. And to close this out here…

**Chalene Johnson:** Yeah?

**Darren:** …so you don’t just freak out and think, “Oh, I’m screwed. I don’t know what to do. They’re going to get me.” You know, like I said before, these guys are smart. You have to commend them for their abilities. But you don’t have to make it easy for them.

**Chalene Johnson:** True.

**Darren:** So, don’t neglect what we talked about today. Share this with your friends, your family. Help them do the same thing. What I want you to remember is this is not difficult. You can do this.

What’s hard is remembering a bunch of passwords written across notes all over your desk and trying to keep track of all that stuff. So, its’ easy to remember one. The moral of the story here is that if you wouldn’t say it out loud with someone in real life, don’t do it online. Keep your information private, secure.

Again, you are invaluable. Your intellectual property is your worth. Protect it like your life depends on it.

**Chalene Johnson:** Gosh, Darren, such good advice. I mean, this has been such an eye-opening slap in the face. I can’t even tell you how schooled I’ve been, like literally schooled in trust. Because your brain just doesn’t work that way, right?

Like I just - I’d never imagine anybody - I’m a nice person. Why would you do that, you know? And what I’ve learned is that it’s happened to people who there’s no one even knows who they are or it was just - it was just out there, so it was fun to grab.

**Darren:** That’s right.

**Chalene Johnson:** And that’s why it’s not an issue that just affects people with a big YouTube account or an Instagram account or, you know, a banking executive. It’s everybody because it’s out there. And we’ve got to be diligent because, as I understand, so much of this has changed in just the last three months, which means it’s going to continue to change, which means y’all need to listen to the next episode.

And Darren, once again, huge debt of gratitude. Thank you for doing this. Thank you for being so…

**Darren:** Thank you.

**Chalene Johnson:** …interested in this and sharing what you know and helping to calm me down and understand this culture and how this happened and what I can do better.

**Darren:** You’re most welcome. And thank you for having me on. And I look forward to being back for part two.

**Chalene Johnson:** Hey, you got it. Obviously, this is the tip of the iceberg. You know, what’s a bummer about all of this, is if I’ve just taken some time and taken these precautions when I knew about them, I could’ve avoided all of this.

My friend, Louis Howes, did a podcast back in, I think, February with a cyber expert by the name of Mark Goodman. I remember listening to that episode and thinking to myself, “Yeah, I need to do some of these things. That sounds important. I should do this.” And I changed a few passwords and I stored them in the password management program and I thought, “You know, how much of a priority is this? I mean, does anyone really ever going to hack me?” Boy, was I wrong.

That kind of thinking is so outdated. It’s so dangerous. It’s so self-centered. People who get hacked are just random names and numbers. Half of the time, the people who have their information exposed really have no relationship or even affiliation with the people who hacked into their information.

If you didn’t listen to the episode previous to this one, go back and listen to it. I want you to hear the panic, the terror and the experience, what we experienced as a family. I shared the really intimate, vulnerable experience because - well, because I want to help other people not be stupid. And there’s no way around it. I was being foolish, naïve. I don’t want this to happen to you.

My friends, check out the show notes, taken action today and check back for my next episode. Darren has promised to give us those next steps as soon as we can record.

I love you, guys. You are the bomb.com.

**[END OF RECORDING]**