**HOW TO PROTECT YOURSELF AND YOUR FAMILY ONLINE**

**Male speaker**: Welcome to The Chalene Show. Chalene is The New York Times best-selling author, celebrity fitness trainer, and obsessed with helping you live your dream life.

**Chalene** **Johnson**: Darren, thanks so much for coming back on the show. You’re like my most popular and most demanded guest at the moment.

**Darren Natoni:** You’re most welcome.

**Chalene Johnson:** Yeah. I guess people realize, “Okay, I should probably be taking this far more seriously than I thought I needed to.” So, if I can, can I just rapid fire ask you questions that people have been asking most frequently on my Facebook page?

**Darren Natoni:** Sure.

**Chalene Johnson:** Okay, cool. So - and, you know, we’re going to talk about things that people need to know. This isn’t like high level security, this is just basic still. These are basics that most people don’t have in place and we’re going to go there today. But just to give people their quick answers to questions, let’s just start with the most popular ones that have come in on Facebook.

All right, here they are. Number one, security questions. They are the same on almost all my sites, at least, you know, like in terms of, you know, your mom’s middle name, those sort of things. How do I get around that?

**Darren Natoni:** Well, just because they’re the same on all those types, does that mean your answers have to be the same? No. So, what did we talk about last time? We referred to not answering them honestly.

**Chalene Johnson:** Okay.

**Darren Natoni:** We need randomize those answers and use generated passwords for them. So, use your password manager to generate that answer and that way you don’t even know the answer. Therefore, somebody else is unlikely going to guess that answer.

**Chalene Johnson:** Okay, cool.

**Darren Natoni:** And then if you don’t do that, just don’t answer them honestly.

**Chalene Johnson:** Now, for me,that used to - so I’m going to speak on behalf of my lifer because they’re like me. They’re like, “I can barely remember my own kids’ birthdates, let alone all this stuff.” So, y’all, here’s the deal. That’s why you have to have a manager, an application that manages all this for you. You don’t, nor should you even try to remember these things. They will be generated and stored in your manager, your password manager.

Second question, “I think my passwords are pretty strong. But how much of my stuff is at risk? Like, do I really need to protect myself with as much stuff as you and Chalene have been covering?”

**Darren Natoni:** All of it. It is all at risk. And I know that sounds intimidating and scary, but in reality, it’s true. That’s the whole point of what we’re talking about.

**Chalene Johnson:** Certainly.

**Darren Natoni:** Any activity that you conduct online is essentially at risk. That’s why it’s important to protect it all with the maximum of the information that’s available to you.

**Chalene Johnson:** Now, I’ve run into so many people since this happened where they’re like, “I get it. But, like, what would they want from me?” And I’m like, “Okay, first of all, your bank account. But secondly, I mean, do you really want the wrong people having the wrong information about you?” And it’s not about, like, whose radar you’re on, it’s just - it can be a database. Am I right?

**Darren Natoni:** That’s right. So, your information is out there, so don’t make it easy, right? We’re not going to make it easy for people to get into our lives. At least put up some level of protection. Take the precautions that we’ve discussed and set yourself up for more likelihood of not getting hacked. You know what I mean?

We don’t want to make it just so somebody can walk into our yard and start perusing through our yard and looking at our house. “Oh, it’s unlocked. Good. I’m going to go in here. I’m going to look through their files. I’m going to look through everything.” That’s essentially what we’re doing.

Nobody would do that in the real world, but because it’s online, they think, “Who’s going to mess with me, right? Who’s going to mess with me? I don’t have, you know, 600,000 followers or anything, so why do I need to protect myself?

**Chalene Johnson:** Mm-hmm.

**Darren Natoni:** But that’s the whole reason.

**Chalene Johnson:** I mean, these kids are after like 50 bucks.

**Darren Natoni:** Yeah.

**Chalene Johnson:** And these are huge organizations that this is the business of hacking into people’s personal information and getting in and getting out. So we have to make it tougher for them.

**Darren Natoni:** Right.

**Chalene Johnson:** Okay. The next question is, how reliable is the password strength ratings that are shown when I’m using my password manager and creating new passwords in these accounts?

**Darren Natoni:** Generally, they’re a pretty good recommendation. Essentially, though, I want you to think about it like this. They’re giving you the answers to the test, literally. They’re telling you exactly what the recipe is that makes the strongest password possible.

**Chalene Johnson:** Okay.

**Darren Natoni:** So let’s say this show 8 to 12 characters or 8 to 21 characters. Do you want to pick 8 when you can pick 21? No. If you’re allowed to use symbols, digits, which symbols, sometimes you might have a problem if they only allow certain symbols, which can be very frustrating if you use like 1Password, for example, in that case and you generate it and you’re like, “Yeah, I’m using digits, I’m using symbols.” But then, “Oh, these symbols aren’t allowed.”

**Chalene Johnson:** Mm-hmm.

**Darren Natoni:** So, it’s kind of one thing we discover with Cox, right? They allow certain symbols. So we had to use those specific symbols and then make it the max.

**Chalene Johnson:** But we don’t have to worry about that because the programs actually read that for us, correct?

**Darren Natoni:** It does in most cases. There’s just that one rare case where they only allow certain symbols…

**Chalene Johnson:** Got you.

**Darren Natoni:** …and the application can’t say to itself, “Oh, I can only use the question mark, the parentheses, you know, the asterisks, something like that.”

**Chalene Johnson:** Got it. Okay, cool. Next, they said - this is a really common one, “Do I need to worry about old sites where I’ve listed my information, or bought things online, or where my information is still there?”

**Darren Natoni:** You mean is your Myspace safe?

**Chalene Johnson:** Dude, I actually deleted mine.

**Darren Natoni:** Yeah. And that’s kind of what I was going to say right there. I would recommend going back, deactivating those accounts that you don’t use because, again, why do they need to be opened? If there’s no reason to be opened, don’t have them opened. But let’s just say you want to hold on to that and there’s an outside chance that one of those platforms becomes the most popular site again in the world…

**Chalene Johnson:** Right.

**Darren Natoni: …**then, go in there and secure it, right?

**Chalene Johnson:** Right.

**Darren Natoni:** You want to secure once and for all. And then we’re just going to not go back to it. We know it’s secured at that point and now we’re going to be notified if anybody does try to get into there.

**Chalene Johnson:** Okay, that’s so good. If I can just share something that I had to do to just - so I could sleep better, right? And that was, okay, I’ve got to go through all my old emails and just look for things that I’ve registered for, look for places. And so I started going through old, old, old emails to figure out, okay, where - you know, and that would spark my memory. And then I started creating a master list.

Because instead of going into each one and changing them as I went, I wanted to create just a master list and then decide, okay, prioritize these, where could there be some information that is compromising, and just going through that item by item by item. Just every time I check one off, I feel calmer and more peaceful and more secure.

**Darren Natoni:** Absolutely.

**Chalene Johnson:** Okay, the next one is, “I know my email provider isn’t safe. But I dread the transaction from switching from the accounts that I’ve been using since I was in high school to one that offers more security. Do I really need a safer email? How do I do this? Do you have advice for me?”

**Darren Natoni:** Yeah. So this is funny. We actually talk about this in our talks about social media, and what does your email address say about you. So if you are using Hotmail, AOL, Yahoo, Cox, these ones that kind of date you…

**Chalene Johnson:** Yeah.

**Darren Natoni: …**then, maybe it’s time to move on, right? Maybe it’s time to step into that next era of email. So, do you dread it as much as having all your information exposed? Think about that.

**Chalene Johnson:** Right.

**Darren Natoni:** Do you really dread that one Sunday you’re going to spend kind of taking the time to do this while you watch TV as much as you dread having all your stuff given to the world out there?

**Chalene Johnson:** Right, right.

**Darren Natoni: [As a matter of fact 0:07:40]**, right? I think you can do it.

**Chalene Johnson:** So true. And, you know, I think we have to just realize the sooner you do this, the better. It’s like that person who starts hoarding almost. Like you just keep bringing things home and you’re like, “Yeah, I’m going to clean out the garage someday. Yeah, I’m going to clean out the living room someday.” You just bite the bullet and clean it one room at a time. You know, that’s the key here is to consistently go through this and take on new practices and habits.

The next one, this is a really popular one, like everyone has texted, called me, I’ve seen this on my Facebook, Twitter, “Are the password management software programs, are those hackable? Like, you know, I’m putting all my information in one spot. Isn’t that kind of scary?”

**Darren Natoni:** Of course. And, yes, it is, given the right amount of time. So, I will…

**Chalene Johnson:** What does that mean?

**Darren Natoni:** Well, think about it like this. A computer can just be dedicated to literally trying to deduce your password. And let’s say that computer is just literally just plugging numbers, going through, boom, boom, boom, just constantly, constantly, constantly, until it eventually figures out, oh, there’s the first character. I got the first character. And then it moves on to the next.

**Chalene Johnson:** Mm-hmm.

**Darren Natoni:** But with 1Password, I’ll just give it to you right from them. So, even if someone were to break into your cloud servers and acquire a copy of your data file, say that was from iCloud or Dropbox, it would be extremely difficult, right? Approaching impossible in a human lifetime for them to actually gain access to your passwords without knowing your master password.

And this is why your master password is so important. Do not make it that same password that you use to secure every other site.

**Chalene Johnson:** Yeah.

**Darren Natoni:** Don’t do that. It needs to be long enough, complicated enough, use symbols, use capital letters, lower case letters. Think of everything to make that complicated but not so hard that you can’t remember it or type it frequently.

**Chalene Johnson:** Okay.

**Darren Natoni:** So, since that literally secures your digital life. So, if you forget it, you’re screwed.

**Chalene Johnson:** How often would you change it? True.

**Darren Natoni:** You know, it’s kind of up to you. If you feel that’s its very secure, maybe you don’t change it as often. But if you’re like, the more I learn, you know, this is probably not as secure as I thought it was to use my dad’s birthday or my dog’s name or something like that.

**Chalene** **Johnson**: Right.

**Darren Natoni:** So, really, as you get more confident in this arena, as you get more comfortable, try to see if you can test yourself. These all can become like little memory games, right? So you’re challenging yourself, “Can I make this a little more difficult and commit this to memory and make this my password?” Our overall goal is to get more and more secure.

So, when I first started out with this, I think my password was a lot easier than it is today. I remember I changed it to - I probably change, you know, every six months or so. So, it really depends on the person.

**Chalene** **Johnson**: Yeah.

**Darren Natoni:** But I recommend using a very secure password. Do not use something that anybody could guess. We’re not using names here. We’re not using that kind of stuff. Think about how to complicate something or put things together in a way that you will understand and you will commit that to memory. But not so someone else could sit down and go, “Hmm, you know what, I know they love Full House, let’s try Danny Tanner, you know.”

 **Chalene** **Johnson**: That’s so funny. Okay, that’s great. Okay, so this really helped me when you were walking me through this process, is you said, “Chalene, from now on, four passwords,” because it’s really not just one, right?

**Darren Natoni:** Right, right.

**Chalene** **Johnson**: So, you said, “Here’s the deal at least for now, for the next six months, until things change again, four passwords. Not a hundred, not two, four. And they were, you told me, my iPhone which we set up to recognized fingerprints, right?

**Darren Natoni:** Right.

**Chalene** **Johnson**: The second one was iCloud.

**Darren Natoni:** Right.

**Chalene Johnson**: The third one was, I forget.

**Darren Natoni:** So, your computer password.

**Chalene Johnson**: Oh, I know, yeah, my computer password.

**Darren Natoni:** Yeah.

**Chalene Johnson**: And then the fourth one was the master password that you have for your protection, whatever software program you’re using, LastPass, KeePass, or 1Password.

**Darren Natoni:** Right. So that might be less for other people, right? So, for you, that’s how many. So, if somebody doesn’t own a computer and they just live in the world of smartphones and tablets, then they might not have to remember a computer password on top of all that.

**Chalene Johnson**: Mm-hmm.

**Darren Natoni:** So, instead of…

**Chalene Johnson**: Who would that be?

**Darren Natoni:** You’d be surprised how many people…

**Chalene Johnson**: Yeah.

**Darren Natoni:** …just own tablets or just own phones because they’re so powerful these days. Again, we live in this digital world where we’re making everything easier and everything is in a cloud. So, if everything is in a cloud, where do you want to go?

Do you want to go try to rob somebody’s house or go to where their actual important information is in the cloud? It’s way easier to get in there. So, think about it.

**Chalene Johnson**: And this wasn’t a question that came up very often on my Facebook page but it’s one I’ve discussed with friends. And that is, most of their kids are all using their iTunes sign in and iClouds and just like, you know, downloading apps and playing games the parents don’t know about. And, you know, logging in using their parents’ Facebook just so they have like access to this app or this game.

**Darren Natoni:** Right.

**Chalene Johnson**: And do you have an opinion there?

**Darren Natoni:** I do.

**Chalene Johnson**: Okay.

**Darren Natoni:** I do. And it used to be more complicated until recently, especially with iOS 8, you know, if we’re talking from the Apple ecosystem here.

**Chalene Johnson**: Mm-hmm.

**Darren Natoni:** So, back then, people wanted to share their music purchases. And they wanted to share those apps and they wanted to share all those stuff. So what people did was they shared one iCloud account.

**Chalene Johnson**: Mm-hmm.

**Darren Natoni:** That might sound familiar to some of you out there.

**Chalene Johnson:** Yeah.

**Darren Natoni:** So, what that’s doing, really? I mean, it’s opening you up now to all the insecure things that every one of those family members are doing. I’m not saying they’re irresponsible, but think of maybe an eight-year-old…

**Chalene Johnson**: Yeah.

**Darren Natoni:** …doesn’t have the same level of experience and ability to judge circumstance as does a 50-year-old.

**Chalene Johnson**: Right.

**Darren Natoni:** So, do we want to give them full access to everything? Probably not the best idea. So, if you have an iPhone or an iPad or a Mac, turn on what’s called Family Sharing. So, someone in the family will be the family manager. They will actually be able to add up to six people to share all those purchases. So you’re talking about your music, talking about your apps, all these things like that.

**Chalene Johnson**: Okay.

**Darren Natoni:** But you can set up parental controls. You can define their ages. You can set it up so people have to actually request to purchase an app from you. And you’ll get a little pop-up that says, “Sally would like to buy whatever it is.”

**Chalene Johnson**: Yeah.

**Darren Natoni:** Whatever cool app it is. And then, you just either approve it or no. You don’t want her doing that, so you don’t approve it. And this also helps - you know, we’ve heard those horror stories - in-app purchase horror stories, right?

**Chalene Johnson**: Yeah

**Darren Natoni:** Where those kids are playing their games and they rack up like a $50,000 bill…

**Chalene Johnson**: Yeah.

**Darren Natoni:** …in purchasing the - stuff like that.

**Chalene Johnson**: I have friends that’s happened to them.

**Darren Natoni:** Yeah.

**Chalene Johnson**: I have friends that’s happened to.

**Darren Natoni:** And so, when they come with that…

**Chalene Johnson**: I’ve had friends like - people just listen to this, you think it’s not going to happen, it does. I mean, I’ve got two girlfriends, both who had young children, download apps, children’s games that thought, “Oh, yeah, it looks fine. It’s a little kid’s game,” to their - what do they call it - iPads, right? And they didn’t realize that the app accesses the camera and then they were playing games back and forth. And in both instances, they were sent pornographic pictures via the game.

**Darren Natoni**: Woo.

**Chalene Johnson**: So, I mean, you just - I mean, just you’ve got - we have to pay attention. Like, there’s creeps out there and there’s weird things going on. And we can’t just go, “Oh, it’s a game called whatever and it sounds like a children’s game. Sure, download it.” Check it out. Look into it.

**Darren Natoni:** So that’s one of the things that I’d really, really, really strongly recommend. Have your own accounts. I’m so surprised how often I come into contact with people who - it’s like even if it’s a husband and wife and they shared an email account, right?

**Chalene Johnson**: Yeah.

**Darren Natoni:** And this is, again, you’re kind of dating yourself there by doing that, right?

**Chalene Johnson**: Mm-hmm.

**Darren Natoni:** Dating ourselves back to time where you had that one email account. Email, especially secure email, is readily available to everybody. So, we want to have our own account because just in case one of them gets hacked, now you don’t have access to the entire family, all the devices, everything, right?

**Chalene Johnson**: Oh, yeah.

**Darren Natoni:** So, that kind of segues into our first topic, really, which is…

**Chalene Johnson**: Okay.

**Darren Natoni:** Email.

**Chalene Johnson**: Yeah.

**Darren Natoni:** The primary rule of email, before we even talk about what services or anything like that, don’t send secure personal information over email, okay? Don’t do that.

We’re going to say that if you absolutely need to send a social security number, something like that, use a service like iMessage, which we’re going to get into in a bit when we talk about phones more in depth. But don’t send secure, personal information. And, I know that’s tough, right, because a lot of times, people are asking for stuff. But don’t include those credit cards and you better…

**Chalene Johnson:** Yeah. And what you do, you go, “Oh, I trust that person, so I’ll just send it to them.”

**Darren Natoni:** Right.

**Chalene Johnson:** But it’s not the person who you’re sending it to who potentially could be looking at it.

**Darren Natoni:** Right. And this is most people wouldn’t pick up the phone and leave a voicemail and says, “Hey, this is so and so. And here’s my credit card information. So, you can go ahead and process the transaction.” Like you just don’t do that, most people wouldn’t do that.

So, don’t do it with your email because that can even be easier for somebody to read, right?

**Chalene Johnson:** Right.

**Darren Natoni:** Right. So, the second thing, the second most important thing, never open a link you are unsure about. Always go directly to the site because so often, people love to hyperlink texts. So they say, “Hey, click here to download this file,” or, “Hey, click here to reset this,” or, “Click here to do something.”

So, what do we do? Well, our brains want to click there. It’s telling us like there, has to click there.

**Chalene Johnson:** Yeah.

**Darren Natoni:** It’s a must. So, you click on it. But, where is it really going? So, what I recommend here is you can mouse over that Click Here link. Typically, if you hold there for couple of seconds, it’s going to tell you exactly what that link is going to. You can actually see that.

So while this email has come in that purports to be Bank of America and you hover over it and sending you some weird random site, hmm, might not want to click on that, right?

**Chalene Johnson:** What do you mean by hover over? And is that the same on the PC as it as a Mac?

**Darren Natoni:** Yeah. So it’s the contextual menu that’s essentially brought up when you hover over something, so like an email address. If you hover over that, it might show you more information.

Or if you’re in your Facebook account and you go to your messages, there’s actually a little shortcut. For those that don’t want to read a message, but you want to see what is in there before you read it to make sure, you know, maybe it’s safe, maybe it’s secure, maybe it’s not, you hover over that text, give it a second. After a couple of seconds, it’s actually going to show you most of that message. If you’re going to hover - yeah.

**Chalene Johnson:** Okay.

**Darren Natoni:** It’s called the hover, you know, kind of the hover over.

**Chalene Johnson:** The hover over. Okay

**Darren Natoni:** The hover over.

**Chalene Johnson:** Love it.

**Darren Natoni:** But that’s what I always do. So, I always recommend hovering over those links that say click here to actually find out where they’re going to go. Or even copy it if it’s not showing up for you and paste it into just a plain text editor, stuff like that. Then you can see, “Ah, this is not going to where it says it’s going.” Don’t accidently click on it, though, right?

**Chalene Johnson:** Yeah, that’s a good tip.

**Darren Natoni:** So just copy that. So, you can right click on that and go ahead and copy that, paste it into plain text editor like TextEdit or something like that.

**Chalene Johnson:** Okay.

**Darren Natoni:** But you can use anything.

**Chalene Johnson:** That’s good.

**Darren Natoni:** So, never open a link you’re unsure about. So, what do you do in that case? You get that email from Bank of America that looks pretty official but you’re just not sure. Go directly to the site. Always go directly to the site. So, go into your browser, actually type in bankofamerica.com. Make sure it actually goes to that and then, you can proceed to do what they want you to do.

But we’re not going to respond to that via the link that they sent us.

**Chalene Johnson:** Okay.

**Darren Natoni:** Right.

**Chalene Johnson:** Got it.

**Darren Natoni:** You got to be also aware that they will often mask this in like an unsubscribe link. To unsubscribe, click here.

**Chalene Johnson:** No, Lordie.

**Darren Natoni:** Are you really unsubscribing? So, really look to make sure that one, those links are going where they say there are. But two, that the email address is actually from the company, the person, something like that.

**Chalene Johnson:** I heard that’s how all of the target employees had - and I’m sorry - customers had their information hacked, is by an employee, a former - actually, a contractor, responded to what they call a phishing email, where it looked like it was from an official source and they clicked on it and sure enough, that’s how they gained access into the system.

**Darren Natoni:** Well, that’s how easy it is, right? So with…

**Chalene Johnson:** Dang.

**Darren Natoni:** …one person’s negligence can now just mess it up for everybody.

**Chalene Johnson:** Well, like, this is weird because, you know, what I teach is email marketing, obviously, and teaching people to grow their businesses in social media. And we do this all the time. We send emails where we have embedded the link into...

**Darren Natoni:** Right.

**Chalene Johnson:** ...the text. So, do you think it’s going to be a more common practice to say, “Here is the link,” so that people can actually see it instead of just hyperlinking?

**Darren Natoni:** Yeah. Yeah. I’m finding that a little more. It depends who I’m talking to. So, this is also why I look at the actual recipient to, like who is sending, the sender? Who is...

**Chalene Johnson:** Right.

**Darren Natoni:** ...sending that email?

**Chalene Johnson:** Okay. That makes sense.

**Darren Natoni:** So look at that.

**Chalene Johnson:** So, especially when…

**Darren Natoni:** Make sure if I get a message from your, Chalene, and...

**Chalene Johnson:** Yeah.

**Darren Natoni:** ...it says - and I actually hover over that and it’s from Kim and some convoluted domain, it’s probably not you, right?

**Chalene Johnson:** Right. Right.

**Darren Natoni:** So, why would I want to respond anything inside of this?

**Chalene Johnson:** Right.

**Darren Natoni:** I would then want to flag it as spam and send to the spam folder.

**Chalene Johnson:** Yeah. Okay. Good advice. That’s going to change the way I think we communicate with your customers, too. I mean it just makes sense, we got to change practices.

**Darren Natoni:** Yeah, you have to adapt, right? You got to adapt.

**Chalene Johnson:** Right.

**Darren Natoni:** Unfortunately, we have to. **[Inaudible 0:21:27]**.

**Chalene Johnson:** Okay. Now, what about these people who have AOL and Yahoo and accounts that they’re like, “I’ve had this since I was in high school. Do I have to delete all of these emails? How do I get my new email out to people?” Like, how do they handle that?

**Darren Natoni:** So, the process can seem intimidating upfront. Until you actually, just sit down and realize, “Okay. This is doable, right?” I’m going to step into the next generation of email. I’m going to leave that AOL behind and I’m going to setup a Gmail account. Now, I recommend Gmail. Why do you think I’d recommend it?

**Chalene Johnson:** Safety.

**Darren Natoni:** Safety, right? So, it automatically has all the latest features. Everything. They update it constantly and a lot of good technology behind it, but at the same time, it’s very safe because of two-factor authentication. But again, when it comes to email, you’re only as secure as the information that you use to set it up. So for giving them crappy security questions, we’re not turning on two-factor. We’re using just a general password, like your dog’s name, then it’s going to be secure. So, you have to use the tips that we’ve given you up to this point to setup the email securely.

**Chalene Johnson:** Okay. So I get it. So what you’re saying to us is it’s not that Gmail is that much safer than another program per say, unless you’re using all of the tools that Gmail makes available to us to secure it.

**Darren Natoni:** Correct.

**Chalene Johnson:** Okay.

**Darren Natoni:** Now, the process of actually migrating can seem very intimidating.

**Chalene Johnson:** Okay. Let’s go there.

**Darren Natoni:** And I understand and I appreciate that.

**Chalene Johnson:** Because people need to do it.

**Darren Natoni:** Right. So, what I like to do. Setup that account, first. Now, when you’re setting up your account, think of the name you want to use. Maybe, this is the time too to kind of step into that more modern, professional email than having, you know, sarahlovessoccer or something like that.

**Chalene Johnson:** Right.

**Darren Natoni:** This might be the time to use your name, use like john.doe or something like that.

**Chalene Johnson:** Well, that’s when they ask, “Is it a - should you have - should you use your name, because that’s really easy to guess?”

**Darren Natoni:** It is easy to guess, but also, having an address that represents you professionally can often times, you know, outweigh that. We’re going to do everything else right so that we can still have that professional looking email.

So when you’re sending messages, you aren’t being judged on, “Oh, well, now I know, she loves soccer because Sarah in her name - and oh, or 87, that’s the year...

**Chalene Johnson:** I see.

**Darren Natoni:** ...of her birth. How many people do that? They always use like, their first name and then like 86. They were born in 86. And then...

**Chalene Johnson:** Or the year they graduated from high school.

**Darren Natoni:** Yeah. They use this very memorable numbers and they put that in something that’s now being broadcast to the public every time they send an email message.

**Chalene Johnson:** Should I have more than one? Like, for - like, so - should I be using one when I’m shopping? And one that only my, you know, intimate friends know?

**Darren Natoni:** I love that you just asked that question. So, before we step into that, let’s finish the migration.

**Chalene Johnson:** Okay.

**Darren Natoni:** So you’ve now chosen your email address. And you have set it up, you know what to do, you’re going to use two-factor, you’re going to use like codes to generate and send to you should anybody try to log into your account, you’re going to have all this setup correctly, right? But now, what about that AOL account?

What about all the messages and all my friends and everybody? So, go into that account and turn on forwarding so that those messages now forward to your new address. Those messages will now forward every email that comes in to that new address. And you could set it up. It depends on who your email provider is, but oftentimes, they let you discard the incoming message after it has forwarded, so your box doesn’t just get littered with all the email.

**Chalene Johnson:** Right.

**Darren Natoni:** They’re overwhelming. After a period of time and once you feel everybody has the right email address, now you can go back and close that out if you want to because again, why are we leaving inactive account open for somebody to potentially get into later?

**Chalene Johnson:** That makes sense.

**Darren Natoni:** Yeah.

**Chalene Johnson:** Okay. So you’re not putting your new inbox at risk by forwarding emails that are going to an inbox that someone might be able to hack into?

**Darren Natoni:** No. And that’s a nice transition to having multiple email addresses. So, if you have something - like if you have your own domain, for example, like chalene@chaleneiscool.com.

**Chalene Johnson:** Right.

**Darren Natoni:** And at the chaleneiscool.com, you could have multiple forwards all going to your actual account. So you could have banking at chaleneiscool.com, travel at chaleneiscool.com, whatever. And for each one of those services, you could have that forward which sends to that primary email address. Basically, it’s protecting or masking your email address. What’s nice about Gmail and many of the other services is they allow what’s called aliases.

So if you have iCloud now, you can actually log into icloud.com and go check this out in your mail setting. You have the aliases. So you could have an email address like timcook@icloud.com but also say timlovesfood@icloud.com, could also forward to that account. So you’re allowed to setup multiple email aliases which will work just like an actual address that all come to your inbox.

It’s a nice feature. I like the way that they **[input them 0:26:30]**.

**Chalene Johnson:** So would you recommend that I create an alias like, for example, one for shopping and that we create an alias for opting into news letters or freemiums, et cetera?

**Darren Natoni:** Right. That’s a very good idea. And the reason is it’s so that if one of those services are compromised, that email address you can just delete it and setup a new one, right?

**Chalene Johnson:** Sweet.

**Darren Natoni:** It makes it easy.

**Chalene Johnson:** Yeah.

**Darren Natoni:** Now, Gmail implements this a little differently.

**Chalene Johnson:** Okay.

**Darren Natoni:** So they have aliases but it’s done in a slightly different way. With Gmail, how you create an alias is whenever you are entering your email address, so let’s say it’s bob@gmail.com. It can bob+whatever it is you want@gmail.com. Adding that plus sign and then any text after that will still forward that message to you, right?

Obviously, if an actual human being is looking at this, they’re going to say, “Oh, okay. Well, I know this is the actual email address and they’re just adding a plus sign to it. But for all those spam bots out there and all those services out there that have your emails, they’re not looking at it from the eyes of a human, right? They’re looking at it from the eyes of robots. So it is then directing that email to you. And you can now know if one of those services has been compromised or given your email account without your permission.

So think about it like this. All the shopping you do on Wal-Mart, you use bob+walmart@gmail.com. One day, you start getting all the stamp from all these different people. But you look and you notice, “Oh, it’s all coming to bob+walmart@gmail.com. Where do you think that your email address was…

**Chalene Johnson:** Oh.

**Darren Natoni:** Yeah.

**Chalene Johnson:** So that’s even better.

**Darren Natoni:** I love it. That’s what I do for every service.

**Chalene Johnson:** Oh.

**Darren Natoni:** And I highly recommend doing it.

**Chalene Johnson:** So with Gmail, you just take your actual Gmail name…

**Darren Natoni:** Right.

**Chalene Johnson:** …before the @ symbol. Add the plus and then whenever you want to stick in there, like you’re at Zappos or Amazon, or whatever. And then that automatically forwards to your actual account.

**Darren Natoni:** Yup. You can go try it right now.

**Chalene Johnson:** That’s so cool.

**Darren Natoni:** It is nice.

**Chalene Johnson:** I love that. That’s brand new.

**Darren Natoni:** So what’s cool about Gmail is that they have that nice filtering feature. And their spam engine it’s terrific. So what you do is you just simply say filter. Create a filter for that any email coming to bob+walmart@gmail.com. Automatically delete it. Remove it from my spam folder. Then you just start using a different one. And this is a good way to identify the people that are giving your email address a way or have been compromised.

**Chalene Johnson:** No doubt. Oh, I love this. That’s so cool.

**Darren Natoni:** It’s a great thing. Yeah. It’s really cool feature. The only downside of this that I have found in actual practical use is that sometimes, I’m subscribing to an actual newsletter that you did subscribe to, can be a little difficult because that plus sign can have a little issue, like Dick’s, for example, Sporting Goods, it’s a nightmare trying to unsubscribe from that with just plus sign.

**Chalene Johnson:** No, we won’t go there.

**Darren Natoni:** Just a heads up.

**Chalene Johnson:** So Darren, I know we’re coming up on the end of the show. I don’t want to overwhelm people, right? I want us to come in little bite sized chunks, so people can digest it. They can follow through. They can take action today. Again, if you didn’t listen to the previous episodes to this one about cyber security, please go back and start there. These come in in very particular order. And I know we’ve got so much more to cover. So Darren, can I have you back?

**Darren Natoni:** Absolutely. I’ll be back. This is an ever evolving field. And we’re just here to help you, not lose your mind, and do this one step at a time and figure it out. You got this. We’re here for you.

**Chalene Johnson:** Awesome. This episode has been sponsored by courageousconfidenceclub.com. It’s a club that I’ve created specifically to help people who struggle with confidence and insecurities and social settings and just standing up for themselves. Being yourself and feeling good about it, all of us could benefit from having more confidence. I’d love for you to just experience a taste of it.

So please be my guest by going to chalenejohnson.com/confidencetips. Now, if you don’t feel like writing that web address down or remembering to go there later, all you have to do is while you’re listening from your phone, send me a text message. The number is 949-565-4337. And that is for U.S. residents.

Then, just send me the word confidence. And I will send you access to this video. This video will help you to eliminate self-doubt and just feel more confident in any situation, whether it’s work or personal or just your social interactions. Every one of us can benefit from having more confidence.

There, you’ll submit your email address. And I will immediately send to your inbox my latest training video where I teach you step by step how to feel more confident in just about any social setting.

I think you’ll find this incredibly useful whether it’s business or personal or just in your everyday interactions. Confidence is something that makes life easier. It helps you to raise more confident self-efficient children. It allows us to speak our mind, to stand up for ourselves, to do the things that otherwise we are paralyzed by fear, and we just allow our own thoughts to stop us.

By learning how to overcome self-doubt and fear of success, you can become that confident person that others are attracted to, the person you want to be, the person you deserve to be, the person you know is inside of you.

So thank you for checking out my free tools by going to chalenejohnson.com/confidencetips.

**[END OF RECORDING]**