**SIMPLE CYBER SECURITY**

**Chalene** **Johnson**: Yeah. So, if you’re a new listener to this show, you’re probably wondering what type of content you can typically expect. Well, I can tell you that, regardless of whether you’re listening to Build Your Tribe or The Chalene Show, my goal is to always help people. And this isn’t typical, but I feel like it’s urgent. I feel like there’s a reason why this has happened to me. And I’ve since learned it’s happening like crazy in epidemic proportions to people all across the United States, all across the world. It’s kind of huge.

And so, if you don’t know what I’m talking about - well, to briefly summarize - a little more than a week ago, I was hacked. More than just hacked. It wasn’t just my social media accounts. It was my personal accounts. And eventually, things got to a very serious level. And, well, the FBI are involved. There are so many details of this case that I cannot share with you. And I wish that I could.

But I do believe, regardless of the position I put myself in by doing so, I do believe this happened for a reason. And I think it’s no coincidence that I’ve spent so much time building and teaching other people to build their social media presence and using social media to attract people to you. And, well, sometimes you attract the wrong kind of people.

And because this hit so close to home, and I’ve since learned it’s affected so many of you, well, I’ve uprooted my previously scheduled podcast that we’re to release last week and this week. It doesn’t matter who you are, you’re hearing this today as a wake-up call.

Do a Google search, you’ll see that social engineering, hacking into people’s social media and personal accounts, it’s the new online game. And things have changed so dramatically in the last 30 days. It’s why you’re hearing every single day when you turn on the news hackers have taken over a target, the U.S. government, and friends and family members. And in most cases, it has nothing to do with your financial status or your notoriety. It’s a game and the players are anonymous. And we’re making ourselves really easy targets.

In the last week, I’ve spent more time with FBI agents and cyber investigators than I have some of my own family members. What I felt last week was just someone hacking into my Twitter account has taken a more serious turn.

That has inspired me to help you avoid the mistakes I made that left myself and my family vulnerable to the same type of attack that I want you to avoid, because these security breaches are new. They didn’t exist 30 days ago. They certainly didn’t exist a year ago, which might be the last time you changed your password. But, as I’ve said before, this has very little to do with passwords.

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 checked, every account I tried to log in to, I’m denied. I’m like, “Ugh. 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, school 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.

That episode was entitled, “Passwords Can’t Protect You.” It’s my account kind of reliving what happened that night. But so much that I can’t share with you has evolved since then.

However, the blessing in all of this is it’s given me a crash course in online security, or maybe better stated “online vulnerabilities”. And we all have them way more than I ever realized. It’s crazy. And it seems complicated and it seems really overwhelming.

And that’s why, following that episode, I brought you friend and former DEA agent, Darren Natoni. And he shared with us some insights into the mindset of these individuals and really tried to shed some light on how this is happening, why this is happening, and why it’s so critical that we educate ourselves in this regard.

We can’t foolishly think that all this information that we’re putting out there, all the apps that we sign up for, all of the places where we enter our information online, all of the organizations that have all of their information even before there was the Internet, all of it is now online.

We can’t think that we can walk around with phones in our hands and those phones know our location and our banking activities and our online activities and that there aren’t people out there who are watching. They are.

And we can’t trust that software developers who are so eager to sell information about us actually have our privacy in mind. They don’t. It’s up to us. And that’s why I wanted to create this episode today, to do a couple of things.

Number one, keep this at the forefront of your consciousness. Do not dismiss this as something that happens to other people. Don’t put this off until the weekend. Don’t take care of 10 other online projects before you follow-up and take of yourself.

You really have to secure your information, your privacy. And it requires us being educated and, unfortunately, a little skeptical. If you haven’t already, please, forward this episode to a few people who you know need take this more seriously. And that includes absolutely anyone who’s using social media or the Internet for their business. They need it most importantly. They’re the ones who I hope will be the most motivated to make these changes.

But again, you don’t even have to be a regular social media user or even somebody who has a smartphone. Your information is on the Internet because the Internet exists.

So here’s a review of what you need to do, the things you’ll need to take action on today. And these things are going to take some time. I’m not even going to play. I am not even going to sugarcoat it. It’ll take some time.

So you need to set aside maybe an hour tomorrow or 30 minutes tomorrow and 30 minutes later in the week to do some of these things. It takes time to protect ourselves. And that’s why we don’t do it. And that’s where the crooks have the advantage, because they know we’ve been too lazy. And that makes their job really easy.

Step one. First, you must update every device you own - your laptop, your desktop, your smartphone, your iPad, your Kindle. Whatever digital device you have that has apps on it that connects to the Internet, you must update the software. Almost every single software update is released to patch up security holes. That’s step one.

And you need to do that because most of the software that allows you to have more protection only works unless you’ve got updated software on your device before you even download it.

Step two. And again, you want to do this only after you’ve updated all of your software, if you want to download a password manager.

Now, I’ve done my research and there are people out there who love LastPass. There are people out there who love1Password. But if you want the low-down on the top software programs that allow you to not just manage your passwords but create encrypted passwords and two-factor authentication, well, I urge you to listen to the podcast just prior to this one that says how to avoid getting hacked and the first steps to fix it, if you are.

In that episode, we discussed the best software programs and how to use them. After, and only after you have that downloaded and that takes some time to get used to and to figure out where you’re going to write down your master password, et cetera, then you need to figure out if your email program, the one that you’re using, maybe it’s Yahoo or AOL or Hotmail, you’ve got to figure out, “What are the security risks of using this particular program?”

To my knowledge, the very best in the industry right now is Google. Google does offer two-factor authentication. So, you’ll need to follow through and do your best to get the safest email account.

“Now, Chalene, does that mean I then have to get rid of all of my old emails or I should tell people to stop emailing me there?” No, there’s ways around that and we’re going to talk about that in my next and upcoming episode with Darren Natoni.

But after you change your email, then you have to go in and change your cloud storage. Some of you are using iCloud, some of you are using Dropbox, whatever it is, that’s a very vulnerable target. You may have heard that even this week, the feds cracked down on teenagers who were responsible for leaking private information hacked from the iCloud accounts of several well-known celebrities.

Once you’ve done that, well then, I suggest you go to your phone. You’ll need to set a passcode. If you have an iPhone or an Apple device, it’s wonderful to use the fingerprint ID. Now, I’m really excited to hear that the Android users will soon have the same feature, because a fingerprint is pretty tough to duplicate.

Speaking of iPhone users, be sure to turn off the mail app, if you’re using that in your Apple device. Because that app, at least, in the research I’ve done in the last week, is still a potential security threat. And Apple is well aware of it but that hole still remains. They haven’t fixed it.

Turn off your location services for any app that you really don’t need it. You can always turn it back on if you need it for Yelp or anything else for that matter.

And then, identify which apps you really need and get rid of the rest of them. Any app that is connected to your social media accounts, disconnect it. You don’t want apps that share access to your Facebook, your Twitter, or your Instagram. You really need to log in to their official account from your phone, and don’t allow other apps to share your login. And you know what I’m talking about. When you download a new app and it says, “Enter new registration information or sign up with your Twitter account, or sign up with your Facebook account.”

Those third-party applications make you more susceptible to a hack.

Next is Facebook. And it’s a big one. Log in to your Facebook and set up two-factor authentication. Hurray for Facebook for having this.

Instagram, shame on you for not installing that yet. It makes Instagram really easy for hackers to hack, speaking from personal experience. And I hope, that with all this pressure, they will soon add two-factor authentication, because as you know, Instagram is owned by Facebook. So, we’re hoping it’s just a matter of time.

But in the meantime, log in to your Facebook, change your passwords. You’ll do that by generating new passwords with your new password management software. Very cool. That makes encrypted passwords, then you provide encrypted responses to all of your - what are they called - security questions. For example, “What street did you grow up on? What is your mom’s middle name?” rather than answering those honestly, you’ll create encrypted responses that nobody could guess because they’re not real. And you’ll do that from within your app. It’s just one extra layer.

Now, does any of this mean that you won’t be susceptible to a hack? No, but it’s going to make it much tougher, way tougher.

People want an easy target. And if you are a tough case to crack, they’ll move on to the next person who didn’t take the time to do these things even after they heard this podcast.

I have friends who know what I’ve been going through, who still haven’t done this. How do I know? Because I hacked into your accounts. Just kidding. I’m just kidding.

I know because I know you. And, you know, shame on you. You need to change this stuff because you’re putting yourself and your family and your content and your hard work, you’re putting all of it at risk. And once you know better, you’re obligated to do better.

All right, back to Facebook.

So, you need to look at all of your privacy settings. Not just your like page, but your personal page as well. You want to remove any posts that have too much personal information. Write down all of the apps you have connected to that particular social media and if you can, delete them. Don’t give any additional app access to Facebook unless you are absolutely 100% positive that there’s no way someone can log in to that.

Facebook alone, I can tell you, I probably spent over an hour just cleaning up my privacy settings on Facebook.

Then, there’s Instagram. Now, once you’re on Instagram, phew, you are very susceptible to being hacked. So, what can you do about that if they don’t yet have two-factor authentication? Well, that’s why I urge you to never log in to Instagram unless you’re doing it from your password manager so that you know that the email and the password that you’re logging into are encrypted, number one, and that they are generated by that password manager so that no one could guess them.

Next is Twitter. Make sure that you checked the phone number that you have attached to your Twitter account. Then, you need to update and secure the email that you have attached to your Twitter account. I suggest that you change it to one - to an email provider that has double authentication.

Next, disconnect any and all apps connected to your Twitter. Update your password by using your password manager, that software program that, again, gives you that encrypted response. Scroll through any old posts, delete any posts which have too much personal information. And then, be sure to click the settings that change your phone notifications. That way, if someone tries to change anything in your account, a notification will be sent to the device in your hand.

Now, there’s so much more for us to talk about, but I don’t want to overwhelm you. I want to make sure you do these things. What I’ve given you thus far, it’s going to take you at least 30 minutes. And honestly, that’s a conservative estimate.

But I can’t even begin to tell you how expensive, frustrating, and time-consuming it has been to do this in retrospect. We just have to get in this habit. Things have changed. They’re going to continue to change. We’ve built this gigantic Internet where everything and anything can go online and it’s filled with possibilities. We just never gave enough thought to how to protect ourselves online.

And with so many people getting hacked every single day, not by hackers in basements who can decode code, but by social engineers - kids who are brilliant online and bored. And even if you do all of these things, of course, there’s no guarantee that new techniques won’t come out next week, that new holes won’t be created. But we have an obligation to keep ourselves informed, to educate ourselves, and to do our best.

I’ve made a post to my Facebook like page that’s entitled ‘Ask Your Cyber Security Questions Here’. Under that post, I want you to list any possible question you might have about your online security. I’m going to do my best to get as many of those questions answered for you as possible by talking to a small group of respected industry experts.

Lifers, I love you. Thank you so much for giving me this opportunity. And thank you for believing me and trusting me when I say, “You need to do this.” Thank you for reaching out and saying, “Okay, you’re right. I’ve been putting this off forever, I’m doing it now.” That means the world to me. That makes all of this worth it.

Until we have a chance to speak again, I just want you to know, you are the bomb dot com.

**[END OF RECORDING]**