**PASSWORDS WON’T PROTECT YOU! - HOW TO NOT BE HACKED**

**Chalene** **Johnson**: On June 6, 2015, at approximately 5:30 p.m., I sent the following tweet, “Perfect day. Slept in, watched three documentaries, digested three podcasts, beach TABATA, meditation, oceanfront lunch and shopping with @brettjohnson11.”

I felt grateful and happy, and relaxed, and content. I was wrapped in a towel, just about to jump into the shower. But I decided to hit refresh a few times just to see if anyone resonated with that message. “You got 21 favorites.” It had been the most perfect day.

But then, as I’m positioning my phone on the docking station in the other room to let it charge while I take a shower, a text message comes in from my friend, Natalie.

You’ve probably heard Natalie on the Chalene Show and Build Your Tribe. She’s a social media expert. You probably follow her on Instagram, Facebook, YouTube, Pinterest, or all of the above. She’s also a great friend. And she sent me a rather urgent text message, “Check your Twitter. I think you just got hacked.” I sat there for a moment, just thinking, “I couldn’t have been hacked, I just sent a tweet moments ago. I wonder what this means.”

So, I logged back in my Twitter, and sure enough, I had been hacked. I tried to think what should I do first. And my instincts were to log back into Twitter and change my password. So I did that, very quickly. And then I thought, “Okay. So, now I have to access my email address, and I should probably change my email address too.” So, I did that.

My heart is raising now because I realized that this person is sending tweets like mad. And at the same time, he starts taunting me in social media. And it seems as though he’s a got ring of friends who are all in on this together. And they’re all retweeting the same comments. And they’re retweeting the comments and @mentions from my followers who have now picked up on the fact that my account has been hacked.

And he’s suggesting all these other people that people should follow. And he’s doing so from my account. And the tweets looked odd, but not so odd that people wouldn’t know it was me yet, not yet.

And it was kind of a panicked feeling because I just - I couldn’t get him out of there soon enough. And I was deleting his tweets as soon as he was tweeting them. And I couldn’t figure out how was I able to delete him and at the same time he was still able to tweet from my account.

But once I changed the password and changed the email, I thought, “Okay, I think I’m safe.” I wasn’t exactly relaxed yet, but I felt like at least I had my Twitter account back. And now I could go back and change all of my other passwords.

But before I could do that, I started getting other text messages from other people who are allegedly in this ring of hackers. And one of them tweeted at me, “I hope you’re watching. I now have control of your over 400,000 Instagram followers.”

I felt the blood rush from my body. I felt panic. I felt nervousness. I felt anxiety. I felt like my head was going to explode. I felt out of control. I felt exposed.

And sure enough, I logged in to Instagram, and they had already taken over that account. They had already changed the name of the account, were deleting photos and adding their own. And now, they’re back in Twitter. Now, they were on my Twitter account, reassuring my followers that my account had been hacked, but that I had control over it again. But yet, it wasn’t me sending those tweets. It was them, as me.

Now, I’m terrified. I’m logging into my accounts trying to change passwords, trying to change emails, and it just keeps kicking me out.

“Oh my God, Oh my God, Oh my God, Oh my God Oh my God Okay, stay calm. Okay. Stay calm. Just stay calm, stay calm,” I keep telling myself. And I haven’t yet told Brett what’s going on because we’re just a couple of minutes into this, and I don’t know what to do yet.

I don’t know how to ask for help. I don’t know who to ask for help. I don’t know where to go. I don’t know what to do.

I tried to calm myself down and think, “Okay, what account do I need to check, first? How can I stop this?” But every account that I check, every account I try to log into, I’m denied. I’m like, “Ugh, shit. Oh my god.”

Then, I would try another account. “Oh my God, Oh my God. No, no. Shit. Oh my God, Oh my God, Oh my God, Oh my God, Oh my God. What do we do? How can this be happening? What do I do? Who am I supposed to call? It’s a Saturday night. How do I stop this?”

Now, I’m really freaking out. My heart is pounding. And I just keep thinking myself, “Oh my God. What are they doing? Why are they doing this? Why is this happening? What do they want? What are they going to do?”

Okay. Take a deep breath and think about what account you need to protect first.

I’m sitting there, trying to focus. What is my next step? And now, my phone starts going crazy, like everybody is texting me. It just keeps buzzing and buzzing and buzzing, high school friends, past employees, friends of friends, business associates, relatives.

“Chalene, you’ve been hacked,” “Chalene, do you know you’ve been hacked?” “Yow, Chalene, check out your Instagram,” “Dude, what’s up with your Twitter?”

“Oh my gosh. Chalene, I think someone’s hacked your account,” “Hey, are you sending these tweets?” “There’s someone in your account, Chalene, quick, check it out,” “Dude, check out your Instagram.”

“Oh my God. What’s going on with your Twitter?” “Chalene, does someone have your phone?” “Chalene, what’s going on? The last three months of your Instagram post just got deleted,” “Dude, you’ve been hacked.”

I couldn’t do anything. I, literally, couldn’t even use my phone. It was still confusing. I just - I didn’t know where to get help next or how this is happening or what was going on.

And all the while, I knew that the hackers were trying to communicate with me. And so I felt like I needed to watch their Twitter accounts. And there were bunch of them. And I was screenshotting them. And I was really just trying to figure out why are they doing this and where are they going next, and who’s involved in this, and what do I do, and what do they want, and how do they do this.

By now, I’m just mental cave. Trying to stay calm, I called Brett upstairs and tried to explain to him what I thought was going on. And I blurted out a few names and said, “Catch these people. See if they can help. Find out if this person knows what to do. Help. We’re really under attack right now. I don’t know what to protect or how I can protect anything. I just - I don’t know what to do.”

At this point in my story, you can probably feel that panic yourself in what we we’re going through. And it gets worse. So, before you dismiss this as a tale, it only happens to people with large accounts, or high profile, or people who spend a lot of time and really rely on social media. I can assure in the last 24 hours, I have learned that is not the case. I want you to know this is your story.

Law enforcement, social media consultants, and cyber-security experts have all confirmed for me that this is a crime that’s reached epidemic levels in recent weeks. And that’s why you must recognize that my story could be your story.

This is the fastest growing cybercrime. Specifically, in this instance, they weren’t your typical type of hackers. Not the type of hackers who crack codes, but a group of hackers who call themselves social engineers. This is the fastest growing cybercrime.

And well, yes, there are those hackers, like the ones who attacked mine who are interested only in selling big accounts. They’re interested in selling accounts on Facebook, YouTube, Twitter, Instagram, et cetera, for a premium.

But at even greater risk is the everyday average internet user. The person who they assume isn’t going to call the police. The person who they think they can dupe or extort fees from. The person who they assume doesn’t know a lot about technology or security.

They do so by what’s called social engineering. All they need is to gather enough information about you, and work diligently to crack the code on just one password for one email.

Or in some cases, that email can be purchased on websites, websites where you filled out applications, applications where you’ve listed your email address. Those websites often sell our personal information more than you can possibly even remember or recall yourself about your own history. It’s all contained in one nice, neat little package, a package known as your history. And it can be purchased on just about everyone for as little as $9.

Once they have this information, most of these social engineers now have enough information to continue following you and your friends, and associates in social media, all the while collecting more personal data about you until such time that they comfortable guessing.

But they’re not guessing your password. See, that’s where we’re wrong. So many of us think that we’re well protected because we’ve been so good about creating complicated passwords and different passwords for each account. But you see, that’s not what they’re guessing.

What they’re guessing is our security answers. What street were you born on? The name of your first pet. That city did your parents meet in? What was your childhood nickname? Which phone number do you remember most from your childhood?

What city were you born? What high school did you attend? What’s your favorite movie? What’s your mother’s maiden name? What was the make of your first car? What’s your favorite color? What’s your father’s middle name? What was your high school mascot?

And they don’t need all of these answers. Usually, they just need two or three. Most of which, they can glean from past records, or ordering the records of your parents, or just paying close attention to what you’re posting in social media.

They do this as a sport. They create additional fake accounts and begin interacting with your friends and family and followers. And if they can’t get the information from you, they’ll get it from somebody else in such a way that you’ll never even realize that’s what they are doing.

I’ll just bet you’ve seen that Facebook post where everyone says, “Hey, list the name of your first pet and the street that you grew up on.” And you’ll have your stage name, if you’re ever to become a stripper.

Or how about when a friend send you an email or post to their Facebook or Instagram or Pinterest, “50 things you probably don’t know about me,” and then, you’re encouraged to send that to 10 other friends. And those 10 friends are encouraged to answer those same intimate questions. Most of which are all the questions that we would use as security answers.

Well, if you’ve ever played that game, you, my friend, were probably targeted by social engineers who now have, perhaps, a dozen or more answers to your confidential security questions. It’s that information that allows people to answer your security questions and hack into your email account even if they don’t have the password.

It’s a sport for them. And once they are into your email account, they can actually see each and every time you would tempt to change a password. They receive the same notifications you do. Now, they can go to all of your accounts and simply click Forgot Password. Then, the prompts are sent to your email inbox, which they’re receiving, and they know the answers to the security questions.

So that was eye-opening lesson for me. It’s not as simple as having an amazing password. It’s more than that. And I’m going to share with you what you must do today, like today. Don’t wait another day. This is what you must do today to protect yourself, your family, and your information.

But before I get to that, here’s what they do next. Their next tactic is to reach out to you, either via cellphone, text message, Twitter, email, Instagram to let you know that they have access to all your personal information.

They’ll explain that they’re the good guys. And in fact, they just want to show you how they found your information and how you can protect yourself in the future. And they don’t ask for much, maybe $50, $200, and explain that you’ll need to deposit into a PayPal or some other account.

Now if you don’t respond to them, what they’ll do next, in many cases, is start sending you crazy, ridiculous, intimately, private information like your past bank accounts, passwords, pet’s names, your parents’ information, the addresses of past and present residence, your income, pictures of your street, every app that’s on your phone.

Once they get into your email account, they can get that information, because almost every application you’ve ever filled out is a public record, leases, the cars you purchased, school you’ve attended, job applications, online services, everything. It’s all out there.

I mean, they really don’t even have to watch you in social media or rely on your friends for these answers. The ones who are lazy, the ones who are willing to spend $9 will simply go to one of these offshore websites where they can purchase your personal information, more than you can possibly even remember about yourself. They can buy it for as little as $9.

Then, they reach out to you and they share the information that they have. And it’s just frightening. And it’s usually ring of them. They hang out on websites and forums. And this is a sport for them.

Social engineers are a different type. They’re different from the type of hacker we regularly see in movies, sitting in a dark room, cracking code. They love to brag about their conquest. Working together under different and fake IP addresses or cloaked IP addresses, which allows them to work together and attack your accounts as you feverishly log in and try to change passwords.

But it’s too late. They’re already receiving your emails. And by now, they may actually be logged in to your laptop or desktop, remotely watching your activity, watching your text messages. And every time you change a password and breathe a sigh of relief, they see it and laugh.

Then, if they’re really cruel, they begin sending screen shots from Google maps to prove that they can see your house, and scare tactics to extort fees. Promising, promising that the only means by which you’ll ever receive your accounts back, the only way to get these hackers to stop is by paying some kind of a fee.

And these social engineers don’t attack during business hours. Nope. They wait until late at night on Saturday and Sundays, when all the customer service reps have gone home, and there’s no way to freeze your accounts.

And many people, when this happens to them, they’ll pay the fees. And you can imagine the panic, confusion and frustration that sets in them. So many people end up paying those fees to these scumbag out of desperation, not sure what to do next. But yet, if you don’t have password scrambling or double authentication on those accounts, and encrypted responses to your security questions, the hackers still have access. That’s scary.

So, what do we do? Hide under a rock? Never use our phones or computers ever again? Refuse to fill any future applications? Live as hermits separate from all technology? Cut a hole in the mattress, and shove our money in there? This week the US federal agency notified 4 million current and former government employees that their private data have been compromised by a massive data breach.

Hackers had managed to break into the US government computers and steal records of millions of employees, making it one of the largest known breaches of information on our federal workers ever in our history. That stolen information included birthdates, credit cards, banking records, security clearances, background checks, dating all the way back three decades. Potentially affecting not just them, but so many of the people they know. I mean, this is a massive breach of security.

I guess the bottom line is this. We’re never completely and fully protected, but once we know better, we have to do better. I didn’t know. Now, I do. And the honest truth is I kind of knew, but I thought it was an inconvenience to use one of these other programs that had provided a two-step authentication process to log in to my main accounts.

I’m too trusting, and I didn’t take the time to figure it out. It seemed like a hassle. It seemed complicated. And frankly, I didn’t realize it was necessary. I thought if I had complicated passwords, that was enough. And not just the computer cyber hacks, but the social cyber hacks, the people who are gleaning our personal information.

So, Chalene what do we do? Chalene, what did you do? Well, I learned a hard and valuable lesson. I lost over 400,000 Instagram followers. And that’s not just a matter of popularity.

Instagram is my brand. It’s my business. Every day I do workshops and webinars, and I speak on it. I teach people how to build all of their social media accounts, but in particular, Instagram.

But, my message is, today, and always has been, that you can’t rely just on social media, that ultimately we need to build our tribe outside of social media because in a snap, just as it did for me on Saturday night, it can all go away.

And at the time that I’m recording this for you, I still do not have access to those accounts. Apparently, they were bought and sold on the black market. And people who specifically wanted to buy big accounts to sell them were able to acquire my account, and Instagram hasn’t been able to help me at all. There’s been so many lessons in this experience.

First, I have to tell you, it wasn’t personal. The hackers didn’t know me. I was just a name on a list. And I ended up on that list because I had a certain number of followers. But these same hackers have attacked people who have only a hundred followers. They just gathered their information, and have been able to extort fees from them, and generally keep themselves entertained by boasting about how they have disrupted other people’s lives.

Yes, I was on a list, but that list included countless other Instagram accounts with a lot of followers. And Youtubers were hacked. All kinds of people who have sizable accounts on social media were also targeted, and their followers sold.

Now, some people were much smarter than me and had that two-step authentication process already installed in their emails and on all of their accounts. And I’m going to talk to you about that in just a moment.

But before I do, I have to make sure you understand this isn’t just about having a lot of followers or big accounts in social media. This is happening every day, by the thousands, to people just like you, who actually have their information online.

If you use a cell phone, if you use a desktop computer, if you have an email address, you just have to anticipate that you will be the next victim. It’s time for all of us to wise up. Even the United States government can’t figure this out.

They’re really no better at protecting us. This is something we have to do ourselves. And even though the attack initially wasn’t personal, it became personal. It wasn’t about my followers, and it wasn’t about the loss of revenue. It was the fact that they knew everything about me, that they were taunting myself and my family, and threatening us. And worst of all, I couldn’t get rid of them.

It took hours, and hours, and hours, and they were still there, a ring of them just taunting me. And all the while I knew they had everything they needed to know to get into our private information. They knew everything. And I thought I had done everything right. And here we were, so exposed, and we just couldn’t get rid of them like parasites.

The second I could regain control over an account, they were back in. I spent over six hours on the phone until 4 a.m. my time, 6 a.m. his time, with a friend, a former DEA agent who stayed on the phone and literally helped me chase them out of my accounts, just long enough to set it up so that they couldn’t get back in.

What they were doing was criminal. And, man, I wanted to catch these little jerks and pinch their heads off. It didn’t take much to encourage me to call the police. I was all pumped up until the dispatcher answered the line. And I said to myself, “Now, how am I going to explain this?”

**Female Speaker:** 911. What’s your emergency?

**Chalene Johnson: “**Hi. Yeah. No, no. This is not an emergency. Yes. Well, I can’t log in to my Instagram account.”

Like that was such an embarrassing phone call. I mean, I had to make it. It was a case of my identity being stolen. And everyone I told what was happening said, “You must contact the authorities immediately.”

And eventually, we had the FBI involved. But that first phone call to the police department was - well, it’s kind of embarrassing once these two big police officers rolled up to my house with squad cars. And both of the officers are not regular social media users.

So, they’re like, “Okay, and what’s the problem here?” And I’m like, “Yeah, so I can’t log into my Instagram account, and all of my content is being deleted, like every picture and every video.” And they’re like, “Okay. So, what is exactly this content?” I’m like, “It’s videos and photos.” And they’re like, “Okay. And so, you don’t have access to these?” I’m like, "Yeah I do. They’re on my phone. But, see, like my followers won’t have” - it just sounded so lame. It sounded so incredibly irrelevant.

But yet, I had to call them, you know. I mean, it really did become a case of someone hacking in to my whole identity. But having squad cars in front of my house on a Saturday night, and then, explaining that to your neighbors the next day, “Oh, Chalene, we saw there were police at your house. Is everything okay?” You know, I mean, what do you say? “Oh, yeah, everything was fine. I just couldn’t log on to Instagram.” #socialmediaproblems. Like I’m sure my neighbors are still, like, laughing about that.

But, you know, I mean, not everyone’s going to get it, but it is a big deal. Like what went down is legit scary. And yes, they’re investigating it. And yes, I’ve notified the FBI. And yes, this is a big deal. But are they likely to catch these guys? Not very. They use fake IP addresses, and cloaked addresses, and fictitious names, and fictitious pictures.

It’s a past time. It’s their sport. It’s what they do to make themselves feel important. Even now, four and five days later, those people who hacked me are still retweeting anyone who happens to mention it, which is why you won’t see me mentioning it much in social media other than to expose them.

But you won’t hear me saying I’m sad about it or I’m bummed or that I feel violated, or how much of a hassle or a nightmare it’s been. You won’t hear me saying that because - well, because it’s not that a big of a deal. I’m over it. And I’m not going to make their day by letting them think they’ve ruffled my feathers. They haven’t.

All they did was give me a great topic for my latest podcast. So, thank you. Thank you very much. Ooh, and you know what else they’ve done? They’ve just made my case. That’s my point. My point is you can’t rely on social media. You need to build your email list, right? Like if this had happened and I didn’t have an email list, I don’t know what I’d do. It would have been a major financial blow.

So, it’s up to you to protect yourself. Trust me, you don’t want this nightmare. I went almost 46 hours straight without sleep. There was no time to sleep.

Every laptop, every phone, every credit card, every source of identity, my driver’s license, self security numbers, passports, bank accounts, licenses, routers, security codes, servers, email accounts, log-ins for all social media, rewards programs, databases, Elance, eBay, Dropbox, Apple IDs, PayPal, websites I shop on, professional associations, membership sites, everything had to be protected. Every computer, every laptop, every online program, it all had to be protected.

Now, I don’t want to profess for even a moment that I am an online security expert. I am not. But, I can tell you this, I’ve had a crash course. And here’s the thing, it is time consuming. It is. And it wasn’t easy. And it was kind of a pain in the butt. But I’ll tell you what, if I could go back in time and do this right to begin with, I would pay anything to have that opportunity.

So, I’m going to tell you two things you must do. You must do this. If you’re a smart person, you will do this. Please, don’t foolishly assume this doesn’t affect you. It does. And here are the two things you must do.

Number one, you must forward this podcast to anyone else you know, who you care about, whose identity matters, including your family members, your spouse, your boyfriend, your brother, your sister, and most importantly, your kids.

Teenagers, and especially pre teens, are using your log in information, or in many cases, your security information to access new apps, accounts, software, et cetera. Everyone in your immediate circle and extended circles needs to recognize that cyber security is no joke.

As a matter of fact, on Monday, June 8th, the United States Army website was hacked. Literally, shut down. None of us are safe. All that we can do is the best that we can do to protect ourselves. So, that was number one. Share this with people that matter.

Number two, you absolutely must download apps to every desktop, and every phone, every digital device that you use on a regular basis that will house and contain all of your passwords in one location. But it’s deeper than that. It’s not just the passwords, as you’ve heard.

The evil side of social engineers who are hacking for sport, they can easily find a way around your craziest, wildest, most inventive system of creating passwords. It’s not the passwords. The passwords are kind of almost irrelevant. It’s your security questions that mean everything, and a two-step process of actually entering into any of these websites.

Now, I know that sounds cumbersome, but it’s actually way easier than you think. It becomes second nature. And it happens behind the scenes once and only after you’ve downloaded these programs and installed it in each of your accounts.

So, we’re going to do this in stages. I’m here to learn this, and I’m here to help you do the same. We’re both students. All you need to do today is download one of these five programs.

Now, I don’t feel as though I’m in any position to tell you which one is the best. I can tell you that I did a little bit of research myself, and decided to download the program called 1Password. But there are five programs that just about every website recommends as being the top five.

The key here is having the ability to do a two-step verification process. I will cover that in my next podcast episode. I will walk you through the process, explain what it means, how easy this can be, and most importantly, how critical it is that we all start using this process. Although, it doesn’t guarantee that we’re safe from hackers, it’s certainly one extra layer of protection, and everybody needs it.

The most popular password management programs include LastPass.com, Dashlane.com, KeePass, spelled K-E-E-P-A-S-S, dot com, 1Password.com, and RoboForm.com. And again, I’ll include this information in the show’s information section. And you can find that by simply clicking on the little “I” with a circle around it when you’re in iTunes.

Do your research on the site on which one is the best for you, download those to your desktop and to your phone. And I will meet you back here on the podcast to discuss how we can use these to our advantage.

Remember, it’s not just for storing passwords. That’s for 2014. In 2015, we have to outsmart the smarty pants, those bottom-dwelling, no shower-taking, video game-obsessing, basement-living, dark-seeking, life-destroying trolls, who find meaning in their life by violating the rights and privacy of innocent people.

Chalene, tell us how you really feel.

Lifers, we are coming back strong. And again don’t forget to share this podcast. I want to turn this negative into a positive. I know this happened for a reason. I’m not going to let it defeat me. It’s got met riled up and ready to share with the world what we can do to protect ourselves. And I’m counting on you to help me get the word out.

Now, my hackers are still blatantly bragging about the disruption that they’ve caused. They’re on Twitter and in social media high-fiving each other, and of course, screenshotting and sharing every comment from my followers and from me, et cetera. So, I’m really trying to not mention this at all in social media.

And there’s no way that those losers are the type to listen all the way to the end of the podcast. They’re just not that smart. They don’t have that kind of persistence or patience. So, I’m not going to post anything about this podcast on my Facebook page because I know they’ll see. They’ve been watching my Facebook page like crazy.

So, that’s why I’m really counting on you like never before to please share this episode. All you do is click the little Share button at the top of your device while you’re listening to the show. If you’ll look at the very top, depending on the type of phone that you have, maybe it’s at the bottom. But the Share button looks like a square with an arrow. When you tap that, you can actually text the link to this podcast show to anyone who needs to hear it.

If I could ask you to please share this with five people, I know we’ll get the world out because I just cannot promote this show on Facebook. I don’t want them to know that we know what they know. You got me? Do you feel me? All right.

All right, lifers, I love you. Until we have a chance to spend some time together again, I just want you to remember you are the bomb dot com.

**[END OF RECORDING]**