Episode #19 of Intentional Wealth: Avoiding Cyber Scams with Cassandra Kirby
A Podcast from Braun-Bostich & Associates

Welcome to Intentional Wealth, a monthly podcast where, alongside notable financial professional guests, Private Wealth Advisor and Founder of Braun-Bostich & Associates, Amy Braun-Bostich, delivers useful insights and strategies that help YOU live your best financial life! Remember, when your money has meaning, and your goals are purpose driven you can truly live with intention.

Now here's the host of Intentional Wealth, Amy Braun-Bostich.

Amy Braun-Bostich: Hello and welcome to this episode of Intentional Wealth. I have our fellow partner, COO, CCO and Private Wealth Advisor at Braun Bostitch and Associates, Cassandra Kirby, along with me today to discuss how to know if you've been hacked.

Cyber-attacks are launched at us every day, and we want to discuss the warning signs you need to be aware of when your security has been compromised. Weekly we hear news of data breaches, exposing our personal records and putting our accounts in danger. Because of this, it is a necessity to take protective measures against those cyber scams because dealing with a hacked account is time consuming and stressful. But the sooner it is caught, the better.

Cassie, please tell us where we should start when we start seeing strange charges on our credit or debit cards.

Cassandra Kirby: Yeah. So, if you notice charges on any of your financial accounts that weren't authorized by you might want to freeze or close those accounts immediately. And just keep aware that sometimes hackers will test your account and make small charges. So, you want to keep an eye out for little debits that you notice in the account, because that could be the beginning of a hack or the beginning of ongoing charges.

One thing to keep in mind is that you can sign up for text or email alerts on your debit and credit accounts, so that way that you know instantly when a charge is made. And if you receive that message and it's something that you didn't authorize, you can contact your bank or the credit card company right away and report that fraud.

Amy Braun-Bostich: Well, signing up for those texts or emails, that's a great tip, Cass. It'll help you track spending and you'll be able to take immediate action if needed.

Cassandra Kirby: Yep.

Another tip is that you can create a verbal password on your bank and credit card accounts. So verbal passwords will save time and money and sanity as well as future chaos, because it's another way to secure the account so most banks don't come right out and tell you to request that on your accounts. But this is one of the most important things that you can do. So, you can go right to your local bank and talk to a branch manager and instruct that you

would like this verbal passcode placed on your account for any phone request, withdrawals, newly issued cards, or even for some transfers.

And another tip is when you're giving this verbal passcode personally, when you're withdrawing money, you don't want to say the password out loud. So, make sure that you ask the teller for a piece of paper so you can write it down and pass it to them.

Amy Braun-Bostich: That's a good idea. I can just see somebody going up to the counter, hey, I want to put a verbal password on it, it's moon over Miami, anyways. That's a good idea.

You want to shred anything that you would put your assets that would put your assets at risk. And you can always establish a verbal passcode with us as advisors at BBA. We have clients call the office to confirm email requests to trade, move money, or change account information.

Cassandra Kirby: Right. It's important to be suspicious of unsolicited phone calls, odd emails, and text messages asking you to send money or to disclose personal information. And you also want to be aware of phishing, which is a fraudulent practice of sending emails or text messages that appear to be from reputable companies or trusted individuals when really, they're an attempt to get you to reveal your personal information or even install a virus on your phone or your computer. So be really careful not to click on links or attachments in emails and text messages.

Amy Braun-Bostich: Yeah, I've even been reading about families having some kind of verbal code because, you know, right now AI can mimic a voice over the phone. And so having a verbal password between family members is also a great idea, I think.

Phishing attempts are usually legitimate looking urgent sounding emails or text designed to trick you into disclosing personal information.

Cassie, recently one of your clients unfortunately fell victim to a scam email. Could you briefly cover what happened and how you were able to help him?

Cassandra Kirby: Yeah. So, he received a link from the IRS regarding a charge, and he clicked on the link, and it said that it was somehow related to virus protection and authorizing a continuation of this protection. So, call this phone number that was attached to the link. So, he calls the phone number, somebody picks up, somehow they get him to download software on his computer. And it may have been a couple different programs that he downloaded. While they were on his computer, they were able to gain access to his personal bank account without him realizing it. They tapped into his line of credit, ran that up to the max, and then they were taking money from the line of credit and moving it into his bank account.

And he could see that his bank account balances were going up and the scammer was saying, “oh, I accidentally deposited money into your account. I'm going to need you to pay me this amount back. I'm going to need you to pay me this amount back,” and it really

looked to the client like those deposits were happening. So, the scammer goes on to threaten him that they've got to make this right. He could lose his job. You know, he was really like pulling on his heartstrings. And it ended up that he went to great lengths to go to various branches of his bank withdrawing money, had a courier come to his house at taking significant sums of cash from him at his house. Because this client was, you know, trying to, to make things right.

And it wasn't until later where he realized that, you know, he was being scammed. And he actually ended up calling our office and, you know, they were starting to ask questions about his investment account, with the scammer on the phone, while he was on with our office. And that's kind of when were able to say, this is not right. You know, you need to hang up with this person. And it just went, you know, it went from there where we started doing some of the things we'll talk about a little bit later that you need to do when you've been scammed, when you initially, when you realize you've been scammed. So that was one of the most significant stories that we've heard. But there's been others in the last couple of years too.

Amy Braun-Bostich: Yeah, it's really interesting how scammers can gain trust and then manipulate the emotions and exploit the financial vulnerabilities of other people to steal money.

Cassandra Kirby: Yeah. And the other thing, you know, is he did, you know, the client listened to what they were asking him to do. So, the bank, you know, as far as the bank's concerned, he authorized all of those transactions, and all of those withdrawals. You know, it's, it was done in a way that it's going to be hard for him to be reimbursed.

Amy Braun-Bostich: Yeah. Because he went in and he took out the money.

Cassandra Kirby: And the line was tapped and all those things were done. And it looked, you know, like it was him and it was him, but there was someone on the phone consistently calling him over like a two or three day period until he called our office and, you know, we had him call the police and it just went from there.

Amy Braun-Bostich: Now, he also had insurance protection, like some kind of cyber security policy. Did that ever pay off?

Cassandra Kirby: So, his homeowner's insurance, sometimes your homeowner's insurance will have a rider for identity theft or identity fraud up to a certain limit. And so, we, you know, we had his declaration pages and could see that there might have been some benefit there. So, he's still in the process of the claim where they want a copy of the police report and all the events and what his actual losses were to try and determine if they could, you know, reimburse him up to whatever the limit was. So that's something, you know, to really think about. We've been doing a little bit of research about what kind of coverage that provides, you know, if you're scammed.

Yeah, we had a couple other incidents where, same kind of thing, emails, you click on it, and another client was asked to go out and buy gift cards, read the code off the back of the gift

card, and then the scammer could use that, you know, the value of the gift card. So, there were, and that was the same kind of thing where you're almost being like blackmailed or, you know, forced into to doing this or else, when really there is no or else. But you're put in such a position that you think there is, you know.

Amy Braun-Bostich: Especially, I think, if you're older, or if you have high empathy levels where, you know, you feel sorry for people if they're in a predicament, I think so, it really impacts people that are. Very kind, I think, and thoughtful.

Well, this is all good information. We'll probably do some more podcasts along this line in the future.

Cassandra Kirby: Some, and just like a little checklist of some of the things to think about, like if you've been scammed or you think you've been, you know, you, you really might want to call the police department and just notify them and they'll kind of take a report from you, go from there. I mean, in this case that were talking about, this was an extreme situation. So, you know, it was super important that he started with that police report for a good accounting and on record that it was a legit scam. But then you also want to close out any accounts that you suspect were hacked. You want to change all of your passwords, including, like, your email, all your bank accounts, you know, your credit card law. You should change all the passwords that you use just to be safe in your kid situation.

Amy Braun-Bostich: They actually had him close the bank account?

Cassandra Kirby: Yeah, he had to close both of his bank accounts and open new. If you think your computer has been, you know, if you've downloaded something, you should take your computer somewhere and have it wiped because there could be other malware or things that are still on there that would allow them to, you know, continue to access your personal information.

Amy Braun-Bostich: It's amazing they were able to get into his bank account. I have a hard time getting into mine even though I know the passcode sometimes. So, yeah, they're just really smart.

Cassandra Kirby: And you should also consider a credit freeze. Like you want to notify one of the agencies, you know, Experian, TransUnion, or I think Equifax is the other one. If you notify one, they'll notify the other two.

Amy Braun-Bostich: You can freeze your credit cards too, right?

Cassandra Kirby: Yeah, you can put a freeze on your credit. So that will, you know, keep others from being able to access or open or extend credit. So that's really important. And also just to keep an eye on, you know, the activity in, on your credit cards and in your bank accounts.

Amy Braun-Bostich: And if you're working with parents that are older, this is really

something to keep an eye on because, you know, sometimes they're clicking on things that they shouldn't be clicking on. And I know from personal experience.

Cassandra Kirby: Yes. And usually like the links in your email or the phone numbers, they're not, you know, there's something off about them. You know, it's not your, like a typical link. But you will. You really wouldn't know that, you know what I mean, if you were older, if you got caught off guard for whatever reason. You just, you really shouldn't click on links that you're uncertain of.

Amy Braun-Bostich: My mom gets fooled a lot by you had a PayPal charge of $459. And then she gets upset and I'm like, well, do you even have PayPal? And she'll say no, but, you know, it's upsetting to get something like that, especially if it's a large number.

Cassandra Kirby: Yeah. And there's been like, I've received texts from UPS or USPS. You know, you can tell that something's not quite right about it, but you could see where it looks so real.

Amy Braun-Bostich: Yeah. A lot of times too, you can kind of hover over the email that it came from to see the actual email. And a lot of times it'll be like a Gmail account, which you know is not right.

Cassandra Kirby: Yeah. It's just kind of scary.

Amy Braun-Bostich: Yeah. It's only going to get worse, right? Because the, you know, the ways of doing this are going to be, like I said, the ability to take somebody's voice and then hack it into, you know, asking for money or saying they need help. That's going to get more widespread as AI develops, becomes more commonplace.

Cassandra Kirby: Yeah. And with, like, we use Schwab as our custodian, so they have, you know, if, and also our policy, just Braun-Bostich, is if somebody calls us and they want money, we need to talk to you. Like, we're not just going to take an email from you. And we can't just send it to a new bank account. You know, it needs to be a bank account that's already been verified. It's already been. You've already signed off on the proper paperwork. Especially, like, if you want a wire done, we need to call the third party, confirm all that information. There's been a lot of fraud with wires to false people. And again, it's hard to recoup that closing money.

Amy Braun-Bostich: For mortgages, for a new purchase of a home. There's some fraud there, too.

Cassandra Kirby: Yeah. So, like, after it goes out, it's hard to recoup because you authorized it in the first place. Obviously, if you didn't, that's a different story.

Amy Braun-Bostich: Well, this is all really good, Cass. And we appreciate you referencing your client scam and providing tools for our clients and others which can help them get out of a scam.

Cassandra Kirby: Yeah. It's just important to remember it can happen to anyone. It's easy to get caught off guard. We're so busy, you know, we have so much going on. It's easy to get caught off guard and you get an email, and you accidentally click. It's just, you want to just try to be very aware of what you're doing and who you're talking to.

Amy Braun-Bostich: Yeah. Thanks again, Cass. I mean, this kind of stuff unfortunately happens every day. And thank you for joining us today. If you have any questions or would like to discuss more about how you can prevent your personal information and or accounts from being hacked, please don't hesitate to reach out to us. You can also go to our website to find more related content and you can find us on Facebook, LinkedIn, and YouTube.