

E23_Fraud Protection Tactics to Keep Your Family Safe





📅 Wed, 12/2 2:38PM ⌚ 27:52

SUMMARY KEYWORDS

child, people, fraudsters, information, jose, email, identity theft, identity, questions, protect, website, triangle, account, scam, check, payment, number, verify, recommend, provide


SPEAKERS


Introduction, Jose, Wil, Liz, Terri


-
-  **Liz** 00:00
In this episode, we'll be talking about the types of fraud and cyber threats you may encounter in attempt to steal your identity and even your children's identity. If you want to learn how to detect fraudsters trying to steal your family's personal information and what you can do to protect them, stay tuned.
 -  **Introduction** 00:21
You're listening to Triangles Making Money Personal Podcast, where we engage in real talk about financial matters that affect our community. Today's episode is sponsored by Triangle Credit Union recently voted best credit union in New Hampshire.
 -  **Liz** 00:37
Hello, and welcome to the Making Money Personal podcast. I'm Liz here with Terri and today we have a very special guest, Jose Rivera Hernandez. He's our Vice President of Data Services at Triangle Credit Union. Welcome Jose! Welcome, Terri! How are you guys?
 -  **Jose** 00:52


Fantastic. How are you?


 Liz 00:55
Good, good.


 Terri 00:56
I'm doing well. And we were just talking right before we started this episode that we're very happy today is actually a recording on a Friday. So we're looking forward to the weekend, right? Yeah, a long weekend. That's right.

 Liz 01:11
That's awesome. Jose, we're glad you're here to join us. And we're going to have you talk a little about fraud, cybersecurity, and most importantly, of all, we want to cover a little bit about child identity theft. So there's been a rise in interest in this particular topic from many of our listeners, and we just kind of wanted to bring it back in a discussion and have you weigh in on it.

 Jose 01:32
Yes.

 Liz 01:32
We hope to cover a little about what it is some of the common tactics that fraudsters and thieves use to get information, and then what parents can do to protect their their families.

 Jose 01:43
I'm excited.

 Liz 01:44
Good, good. Because of your experience in it and data services that like we want to have a little Q&A with you, and we can talk about these topics. So you can you know, provide some of your own experience and your industry insight. Are you ready?

J Jose 01:59
I'm ready.

L Liz 02:04
Okay, so child identity theft. It's a growing problem and it's alarmingly one of the many ways that fraudsters and thieves collect and use personal information. So one of the first questions we want to ask you is, there's something out there called imposter scam calls. We're curious to know if you can provide like a little bit of explanation about what these types of calls are, and then what people can do to avoid being defrauded by them.

J Jose 02:30
Certainly, so, you know, email is not the only tool the bad guys use to phish for your information. You know, there's vishing, what is called voice phishing. Those attempts are on the rise, particularly during vulnerable times, such as now with the COVID19 pandemic. These calls vary from scammers asking for donations to a fake charity, giving you fake news updates, and even offering free COVID-19 test kits. The call may come from a phone number that you recognize and maybe even some quite convincing. Once they have you on the line, the call quickly escalates to ask him for your personal information, you know, such as your name, address, payment information, and more. My tip is don't fall for it. What we recommend, you know, I've been in security for a long time. So, you know, what I recommend is never sharing personal information over the phone, especially if you did not initiate the call. Be cautious of urgent requests, like making an immediate payment or being pressured to provide your information, whether it's personal or financial. If you're not sure if a phone call is legitimate, hang up and try contacting the organization directly through the phone number that they have provided you before or go to their website.

T Terri 03:57
Those are awesome tips. Jose, I like those recommendations for sure.

J Jose 04:01
Yeah. Thank you.

T Terri 04:03
Um, so Jose, I have two daughters, and, you know, I haven't done a very good job of

assessing, you know, if anybody's actually ever used their information. What warning signs would you typically see if someone has stolen my child's identity, or information or is using it fraudulently?

J Jose 04:32

And, yes, I have an 8 year old son and I have four kids. Three of my daughters are older and even, you know, back then, you know, we used to be unaware of all this. So many of us know about identity theft and its negative impact on our society today. With many ways, identity theft can occur, it's no surprise that almost anyone can become a victim including our children, right? So, childhood identity theft has been increasing over the past few years, according to a 2018 child identity fraud study by Javelin Strategy and Research, over 1 million children have been victims of identity theft in the past year, and two thirds of the children affected were under the age of eight.

T Terri 05:26

That's amazing.

J Jose 05:27

Oh, yeah, you know, we have kids, I mean, my eight year old son, yeah, I'm concerned about him. Um, but you know, some common types of childhood identity theft are based on what the thief is trying to accomplish. So, for example, financial ID theft, you know, it's commonly a synthetic ID created by combining the child's social security number with an adult date of birth, you know, creating a false identity, many to apply for loans, lines of credit, etc, you name it. Another one I can think of is the tax childhood ID theft. You know, this crime uses the childhood identity information to collect earnings, or to avoid tax liens, or obligations they owe. I mean, it is a some pretty crafty people. And the last one, believe it or not, is the medical ID theft. The thief can use the minor's information to receive medical services, or use it on billing documents or statements to avoid paying for medical services themselves. I mean, I can only imagine now at this moment in time that that's probably something that's rising.

L Liz 06:41

Hmm. Wow. I think it's crazy to think like I, you brought up a good point about we don't, we don't always think of kids, when we think of identity theft. We usually think of people who have established identity, like histories, established credit histories. So it's kind of crazy to think that there are people out there who will attempt to take all these little ones'

information, and then just kind of mash it up together and create, I mean, in the sense of the synthetic identity or something where they generate their own person based on this child's information.

J Jose 07:18
Yes, it's crazy.

L Liz 07:21
I don't have any kids myself, but I'm sure there are a lot of people listening who do so what are some of the things that they can do to protect their own child's identity?

J Jose 07:30
Well, you know, a quick way to safeguard you know, our children's personal data is to freeze, you know, his or her credit. Now, this can be done by calling the three major credit bureaus, Equifax, TransUnion, and Experian. You print out a, you know, child freeze request form mail the request and document the copies. Keep them for your records, you know. Calling them, is a good way to check if there has been a fraud in your child's name. You know, usually bureaus will ask for some type of verification, you know, from us, you know, parents or the legal guardian, in order to verify the child report. And also be selective about who you share your child's social information with. Not everyone who asks for your child's social security information needs it. You have the right to ask. Why is it that they need that that information? How's it going to be used, stored, and protected? I mean, if you're still wary, ask if there's an alternative to providing your child's social security number, which there's, there always is. Another thing is educating your children. Sometimes they give out information without knowing. So educating them by, you know, talking to them and having a conversation about what kind of information they should share with anyone. Teach them about smart Internet behavior. When they see children with iPads and iPhones, teach them how to spot scams and, you know, anything that's suspicious,

T Terri 09:19
Jose, so you know, just in terms of both for my own personal information and account information as well as my child's, what's your should we do if we discover that there's some fraudulent activity on our financial statements?

J Jose 09:39
If you do discover that, you know, I recommend contacting the financial institution as soon as possible. And that's a good point, you have to review your financial statements periodically, all the time. There are institutions out there, reputable financial institutions, that offer services to protect members against fraudulent activity. You know, typically, you know, when discussing the issue with, you know, Member Services, there'll be questions regarding the amount in question, the activity. The goal is to discover the issue and report the problem early. So it can be resolved quickly?

T Terri 10:20
Absolutely.

J Jose 10:22
Yeah. I think, you have to remove those out of your credit immediately.

T Terri 10:27
Yeah. So Jose, so do you recommend like, like a review? Should we be checking either with our online banking or financial statements maybe a couple of times a month or weekly? Like, if you don't mind, I don't know what your recommendation would be on that.

J Jose 10:47
Yeah. So what I have it's a service with our Experian, I believe that I get a report monthly. I can go on any time and review it.

T Terri 10:59
Yeah.

L Liz 11:00
Nice. Okay, so for other parents out there, what kinds of things can do? Or what are some of the ways that they can limit the risk of childhood and he kept on their kids?

J Jose 11:14

Yep. That's a good question. Consumers should be looking for identity protection coverage, like, for example, Triangle's Better Checking account that offers an anti theft, protection for the entire family. The whole family. It covers children up to the age of 25. That's a really good question. In addition, you can consider freezing your child's credit. In that case, like I mentioned before.



Liz 11:41

How would you go about, do you know, any of the steps in particular of how to go about freezing your child's credit?



Jose 11:47

Yeah, so you know, reaching out to the, you can visit the website, Experian. You can go to TransUnion, like I said, I have a report, I have a subscription with Experian and one of the options is to do that with my children. You know, providing them the social security number and freeze the accounts and not only freeze, the account but it provides a report, if anyone has even tried to use their social security numbers, because I'll be honest with you, it's I will say, a lot of the personal information is already out there in the dark web somewhere. It's out there, we just don't know so we have to protect it.



Terri 12:32

Jose, I really appreciate the fact that you just use the word dark web. Can you explain that a little bit? Because I've actually heard that term a lot but I don't know if I truly understand it.



Jose 12:46

Yes. So you know, we have the Internet where everybody can go to the your restaurant websites. Underneath that, there is another, Internet so there's computers connected with each other, where they do not use any names such as www.google.com, what they use is numbers. And in order to find websites, you need to know the numbers. So the only way that you can connect to the dark web, you know, you have to use encryption tools. There's a lot of different tools out there that you can use that way you can connect to the dark web. So you cannot find it anywhere in Google. There's probably ways and instructions on how to connect to the dark web. And you know, the dark web has been known for a lot of, I will say selling drugs and other things that are not commonly sold, you know, on Amazon. So this is why it's called the dark web. You know, and that your identity is it's hidden. Certainly the government has, you know, brought down a lot of the websites that

have been selling things like drugs and other weapons and everything that's illegal. Um, so the dark web is a place also where hackers that have stolen data, personal data, financial data, they're able to sell it through there. So your credit card number, your date of birth, your social security number is on sale right now for maybe for \$5 up to \$50 again, because they're making money each time that they sell it. So they can sell you social security number of 50, 100, 1000 times. Wow. They can sell the same number multiple times? Multiple times. Yes, multiple times I can sell and this is where this is why it's so cheap. You know you can, you can buy a social security number for \$5 and they know that they will make that money over and over again. And certainly if you want a social security number, date of birth and address, then the price increases. Again, a lot of the people that do right now, what I recommend is, you know, we have social media, what I will recommend, highly recommend, is for families not to post date of births, phone numbers, the favorite things of the children, because that's what, you know, the the hacker sees and that's what they're looking for. You know, so we have to avoid that.

L Liz 15:34

Yeah, I think with some of the platforms out there, people are very open with their lives and with their information. And I don't think that we are concerned a lot about what we put out there. I think we think it's protected, it's safe, you know, we have a password or something like that, or I mean, even something public like a birthday. You know, I wonder if maybe, like you said, we should probably all be a little bit more careful about that type of information we even just put out on our social. Because we think we're having fun with it.

J Jose 16:09

Yeah, and particularly now, in during this time is where you feel isolated, and you want to, you know, you want to feel like, I'm still here, you know, don't forget about me, and yeah, you have to be cautious.

T Terri 16:22

You know, that's, so spot on to Jose, because how often can we you know, if we're having a birthday party, it's one of my children's birthday parties or whatever, we'll pop it out there. And truly anybody who's looking and kind of cyberstalking anyone can deduct, like, based on the information that they're seeing, oh, this must be their birthday. This must be their, the birthday date, and you can always kind of tell too how old the child is, you know. Yeah, there is a lot of information out there. Jose, what are some of the tactics that you've seen, that fraudsters have used to get information?



Jose 17:02

So, you know, it's, you know, we mentioned the social media, I'll also say, you know, sometimes when people will probably find them in, you know, you're walking around in the park or the beach, you know, some people are too friendly. What they want to do is build a trust with you immediately. And for some reason, we are attracted to trust people and when we do that, we fall into providing information more than what, they're looking for. If we start talking about our children, you know, they start saying, well, you know, I have a child the same age, and then they start asking about, you know, yeah, my child likes to play Legos. Wow, my child does, too, and so on. Before you know it, we provide more information than is needed. Fraudsters are very, very smart. They come up with some very crafty questions or they know, they see you where you are probably in a moment that you need help, and you're willing to provide a lot of information.



Liz 18:18

Yeah, they'll get you on concern, or they'll get you on fear. And they'll want you to act quickly, right?



Jose 18:24

Mm hmm. Oh, yes, definitely.



Liz 18:27

I've almost fallen for one of those ones, I got an email, and it was from PayPal, not well, not actually from PayPal, but it claimed to be, you know, claimed to be from their support. It was basically saying that there was a transaction that they needed to check or something like that. And I remember thinking, and of course, they wanted me to click a link and view my account. And something inside said this isn't right, you know. So I, I went on PayPal's website and I looked to see if they had posted anything about a common email scam that was going around, you know, and they had on their website, they had guidelines of what they would never do when they send their emails. And one of the things they list is, we will always address you by your first name. In this particular email, it was dear member, or dear customer. It didn't actually have my name. And then PayPal listed a couple of other things as well that you would only expect from them. So then when I did a little more research into the email, I noticed as convincing as the logo may have looked at first, it was not the PayPal logo. And then of course, I hovered over the link as well, and the link had a longer extension on it, you know, so all of those things started to fall into place. But, if I went by what the email had told me to do quickly, because it was kind of alarming.

It would have been too easy for them to get my information. So I've almost fallen for it.

T Terri 20:00
Gotta keep your guard up, Liz, that's for sure.

L Liz 20:02
Totally.

J Jose 20:03
All the time.

L Liz 20:05
Yeah. And I mean, they put in effort to like they made this logo look like PayPal's, but it wasn't. So like, check all of those things in an email.

J Jose 20:15
Yeah, there are those that right now in this moment, and you know, during COVID-19, many people are probably not working. And there's the offers of free money, you know, free credit cards, free gift cards. People will fall for that.

L Liz 20:31
Yeah. They get excited or Yeah, they want to redeem now, or put in their information. Yeah. Going along the lines of that, I mean, if they're, they're looking for, I would guess in many cases, these fraudsters, they want your information or they want some kind of money. What kinds of other financial risks or just in general, what kinds of financial risks are there for falling for email or phone scams?

J Jose 20:57
Well, identity theft is the number one in stealing someone's identity. You can open a line of credit, you know, you could open credit cards, loans. It takes seven years, I believe, to remove a bad account from your credit report. That's a huge impact to someone. Someone who particularly who's young and wants to buy a new car or house. You know, and so that's a, it's a huge financial risk for, for anyone, you know, who falls into this thing.

So whether it's identity theft, or is just not being able to purchase a new car or get a house.



Liz 21:49

I mean, think of the time and the expense of fixing it. Trying to fix it.



Terri 21:55

Definitely. Jose, what's the number one thing that you would recommend to someone to keep them themselves protected from fraudsters online?



Jose 22:07

My number one will be to know your accounts. You know, nowadays people have multiple credit cards. What I will recommend is know what you have, know what the limits of your credit cards are. Know how much you owe, when your last payment was. So in case you get a call or an email from someone attempting to tell you that you did not make a payment, or you went over the limit, you know that it's a fraudster. It is a lie. Because you know, what you have, what you owe. I would say that that would be my number one recommendation to anyone. Get a copy of your credit report. Like I said, there are places where you can purchase a subscription every month and get a report, or you can review it monthly, you can review quarterly. It's up to you, but review it. Get a copy.



Terri 23:10

Yep. Hmm. Sound Advice? Thank you.



Wil 23:15

Hi, guys. Wil, here. We hope you're enjoying this episode and sorry to interrupt but here's a quick word from our sponsor.



Introduction 23:23

Pay people in a snap using Pop Money with Triangle's mobile or online banking. Need to reimburse someone for lunch? Or pay them back for something they bought for you? With PopMoney, there's no need to write a check or find an ATM for cash. All you need is a Triangle checking account, and TCU online or mobile banking to try it out. Setting it up is

easy, and when you're ready to pay, all you need is the recipient's email or mobile number. Don't bother with the hassle of setting up other digital payment accounts when you have Pop Money. Try it out today for a convenient way to pay others or request a payment securely and easily. Visit trianglecu.org to get started.



Liz 24:10

So Jose, we've talked about fraudulent emails, fraudulent phone calls, you know, the ways that these fraudsters try to get a hold of our information. Can you list some of the common signs that people should probably look out for when they receive an email or a phone call? And if they see these signs, what are some of the things they can do to verify that they're either legitimate or not?



Jose 24:33

Sure. So you know, for emails, a lot of the emails that are fraudulent, they have a lot of misspelling. That's the most common thing that I've seen. The dates are wrong. The format of the email is not as professional as you think would come from a reputable company. You know, the sender's email address is not reflecting the company. And one last is the urgency. You know, a lot of those fraudulent emails want you to take action now. The same goes for the phone calls, you know, phone calls, I think they start with urgency. Again, they need you to take action now. They don't want to give you the opportunity to think that it could be a scam. Or another one that is common is the difficulty to understand. Because a lot of the people that call are from other countries. And another one that I notice is their unwillingness to respond to questions. So this goes too. How do we verify if an email or a phone call is safe? I say with a phone call it is, ask questions. Ask them for a number to call back. And usually when you ask that question they're unwilling to give you any number. That's a big red flag. Ask to speak to their manager. Ask about information on what they have about what they're calling for. You know, when you call one of your companies to verify your accounts, they usually ask you questions, right? You know, what's your balance? What's your address, date of birth? So I think we, we ought to have the same right and ask the same questions to them, whoever's calling us and say, What are you calling me for? What kind of information do you have about me? You know, if they ask you a question, you say, you already have that information. Why are you asking me for my date of birth? Why are you asking me for my balance? So that's, what I would do to verify that.



Liz 26:49

That's cool. That's good to know. I wouldn't have thought of. See my first reaction would

probably just be to hang up, but I didn't think about asking questions. You know, because maybe it is something legitimate or not, but that's one way to just test it.



Jose 27:03

Yeah, and if you hang up, trust me, they're gonna call you back.



Terri 27:09

Thank you so much, Jose, for sharing this valuable information with us.



Jose 27:13

Thank you so much for the opportunity. Thank you.



Liz 27:15

Thank you. Jose, we really appreciate it.



Terri 27:16

For our listeners, we hope that you found this podcast on protecting you and your family from fraud helpful. Thanks for listening to Triangle's Making Money Personal podcast today and be sure to check out our other tips and episodes on our website at trianglecu.org. If you have any comments or recommendations for future shows, please email us at tcupodcast@trianglecu.org. Have a great day.