KEEN ON
RETIREMENT

Lock Up Your Nest Egg With These Expert Cybersecurity Tips from an FBI Special Agent

Welcome to Keen on Retirement
With Bill Keen and Steve Sanduski

Steve Sanduski: Hey everybody. Welcome back to another episode of Keen on Retirement. I'm your cohost Steve Sanduski. With me, as always, Mr. Bill Keen. Bill, how are you doing today?

Bill Keen: We're doing good here in Kansas City today Steve. How are you all doing?

Steve Sanduski: Doing fantastic. It's another beautiful summer day here. We've got an exciting show lined up today. We always want to try and bring timely topics into the conversation. We've got another doozy here today, don't we?

Bill Keen: We do Steve. We talk a lot on the program about getting your ducks in a row and having a plan to be able to retire at some point in the future if you aren't already and to make the appropriate tax decisions, date of retirement decisions, investment decisions, Medicare supplement decisions, Social Security decisions, all those things that go into a comprehensive financial plan. Then being able to understand how to find a competent fiduciary financial advisory team that you can trust. All those things are the message we have here at Keen on Retirement during our programs and at our Keen Wealth Advisors.

There's another issue that we thought we needed to continue to talk about on the program. All those things are important, yes, but if someone ends up scamming you or stealing your money all bets are off. We believed that it was important for us to do whatever we could do get the very, very best resources on the program and deliver them today.

Steve Sanduski: I'm just really excited with the special guest here Bill that you've brought into the office with you. His name is Jeff Lanza. Jeff is a retired FBI agent. He was with the FBI as a special agent for over 20 years. He investigated cyber crime, fraud, organized crime, human trafficking, terrorism, he's been all over the national media. He's published a couple books and we're going to chat about one of them here today. He's also consulted for an Oscar winning movie director, Ang Lee. He's presented all of the world including 49 of the U.S. states. We'll have to ask Jeff what's the one state that he hasn't been to yet.

Perhaps most importantly, he serves as a certified Kansas City barbecue judge. He's one of Kansas City's very own. We are very excited to have you here. Jeff Lanza, Jeff, welcome to our show.

Jeff Lanza: Thanks Steve, it's great to be here thank you.

Bill Keen: That was actually the reason we invited him on Steve was the barbecue expertise.

Steve Sanduski: Maybe we just need to start right there. What is your favorite Kansas City barbecue?

Jeff Lanza: It's a place that used to be called Oklahoma Joe's. They took Oklahoma out of the name because it's not in Oklahoma, it's in Kansas City. It's called Joe's Barbecue, it's one of my favorites, not that they need a plug because there's a line outside their door starting about 11 o'clock every morning of their multiple locations, but they are a good barbecue, one of my favorites.

Steve Sanduski: Bill, it sounds like you can probably attest to that.

Bill Keen: I can sir. Next time you're in town we'll have to go over there now.

Steve Sanduski: Sounds great. All right, well Jeff we're going to be talking about this cyber crime, and fishing, and how people are out there trying to get access to our online accounts, and different ways that we can prevent that. I thought maybe the first place we could start is when you say an FBI Special Agent, as we were talking here just before, that almost sounds James Bond-ish, so maybe if you could just start with what does it mean to be an FBI Special Agent?

Jeff Lanza: I often get asked the question if there's a difference between a Special Agent and an Agent, which is basically a representative of the U.S. Department of Justice, the largest investigative agency inside of the U.S. Department of Justice that investigates a wide variety of federal crimes. There is no different between a special agent and an agent. We all like to think of ourselves as special. We actually got the name "special" because when the FBI became an agency they were only allowed to investigate and only had jurisdiction to get involved in cases that they were given to by special authority of the Department of Justice, so the name became Special Agents. Secret Service, who guard the president,

are also called Special Agents, IRS also called Special Agents, as well as DEA Agents. The name is just because of the special designation, that's how it began.

Steve Sanduski: Excellent. Well we do want to talk today about protecting your information. If you could just start with one or two of the ideas here that we all need to think about in terms of protecting our family in this information age that we live in today.

Jeff Lanza: You mentioned cyber crime. I'll get into that in just a second. I do want to mention though because it's such a significant problem today after the Equifax breach of almost a year ago, September of 2017, that's put out Social Security numbers out in the hands of the hackers, over 140 million of those. If your Social Security number is in the hands of a bad guy then they can use it to commit fraud much more easily than if they didn't have your social. One of the ways to keep safe from that type of fraud is to consider freezing your credit reports. Freezing your credit reports would mean if I get your social and I try to open up a credit card using your identity, which is a common thing that criminals do, they won't be able to do it because your credit report is frozen and the credit card company would not be able to get your credit history, so they won't give the credit card to the criminal. Check out credit freezing in the state that you live and do Google searches on that. You'll get information about how to do it, how much it costs, and it's a lock down that prevents many types of fraud. That's just plain old identity theft where someone gets your social and tries to open accounts in your name.

There's many other ways that they steal our information or take over our accounts on our computers, for instance. One of them involves just a plain old email that's been sent to us by a crook, by a hacker, and we click in the wrong place. We click on something in the email, we open an attachment that affects our computer or we click on a link that sends us to a website that ends up causing us problems on our computer. By installing malware on our computer, malicious software, they can steal information or by sending us to pages that look like real pages, like our bank pages, like our email account log in pages. We put our information into log in and that information ends up going into the hands of the criminal. These are the most common ways they steal our information to get access to our online accounts.

Steve Sanduski: I had a situation happen here just a couple weeks ago where I got an email from someone that I know and the body of the email said something to the effect of, "I've got some documents that you were asking for." It sounded legit but they were secured documents and this was coming from another financial advisor. Oftentimes, a financial advisor will send a secure document, but it just looked a little fishy. The name on the email was legit and it was the actual website of the URL, so I replied to the email. I said, "Hey, just wanted to confirm that this was legit." Then within about 10 minutes they replied to me and said, "Yeah, Exactly." It sounded like this is all good. Well then fortunately I got distracted on something else. Then about 15 minutes later I got an email from someone else

at that firm that said, "We've been hacked. If you got an email from us it's not legit." I thought, "Man, these guys are good because I even replied to the email and they responded back to me." That was getting a little sophisticated I thought.

Bill Keen: Oh my.

Jeff Lanza: Yeah they're very good at doing that. What they do is they do hack people's accounts, companies or individuals, and they use their email accounts as a launching pad to send spam, or malware, or to take over other accounts. That's what happened in your particular case.

There's all sorts of tricks that they use to redirect you or you may think you're talking to somebody that you know and it's actually being sent to someone else that's actually the hacker.

The thing that we can all do to stay safe in this is just be careful where you click. Always be careful where you log in to your emails accounts and where you log in to your bank accounts. Make sure you're on the right page for the log in process. Never log in through a link, never log in through a popup or anything that says "You need to log in here to get access to your bank account." Make sure you go to the bank account site, for instance, your financial advisor site, or whatever site you're talking about directly. Make sure it's the right site by hovering over the URL to make sure it's correct and then put your credentials in at that point and time. That's the proper way to log in to make sure you're not getting your accounts hijacked.

Steve Sanduski: We had a situation of course that's been in the news where I believe it was the Democratic National Committee, their servers were hacked as part of some type of sphere phishing process. How did that work?

Jeff Lanza: Right. Phishing emails are where people send out a broad amount, a large amount of emails to try to hook people, to try to catch people in this broad net. They know not everyone's going to click in the wrong place and be victimized, but they know they'll get a few. A spear phishing email is different than that, you'd think it was analogous to fishing. You're not putting out a net, you're sending a sphere, you're looking at person, you're trying to hook them.

What happened in the DNC case is they targeted a person at the DNC and they sent an email to them that looked like it was a problem with their email account, and they had to log in to correct the problem. They clicked on a link and it brought them to a log in page that was not the log in page for their email account. That was controlled by the hackers. When they put their credentials in, their user name and password in the boxes on that page, then the hackers had access then to their email account. That's how they were able to hack into the DNC's email account. That wasn't the only one, it also happened to John

Podesta who was the chairman of Hillary's campaign, he was hacked the same way, almost the exact same way.

What we have to look out for, these are high profile examples, there's people indicted for those things that we just talked about, what we have to watch out for is not falling victim to those phishing or spear phishing attacks to try to hijack our various accounts.

Bill Keen: Jeff I get it seems like every day an email from Apple and/or PayPal. I send them over to Matt here he's been with me 17 years. I introduced you to him here earlier and I say, "Matt, is this real? Is this real? Is this real?" He tells me every day, "No Bill, delete, delete, delete."

Jeff Lanza: Right, right, right.

Bill Keen: It's Apple telling me that I've bought something on my iTunes account or it's PayPal saying there's been something bought overseas. All those do you just delete, delete, delete-

Jeff Lanza: Yeah.

Bill Keen: ... there's nothing else to do really, is there?

Jeff Lanza: Those are good examples because I actually have those two very examples in my presentations about-

Bill Keen: Oh good.

Jeff Lanza: ... cyber fraud. There's nothing wrong with using PayPal and there's nothing wrong with having an Apple ID. If you have an Apple product you have an Apple ID, but what you want to watch out for is those type of emails that try to hijack those accounts. If there's a problem with your PayPal account, there's a problem with your Apple account, you go to the site directly and log in. If there's a problem you'll learn it when you log in with your credentials, never through a link. In fact, the general rule to be safe online is to never click on a link to go to anywhere where you're going to enter your credentials. You're always going to log in, you go to Apple site directly, www.apple.com, www.paypal.com. Save that in your browser as a bookmark so you don't have to type it in every time, never through a link, only to those sites directly to enter your credentials.

Bill Keen: I think that most people don't realize how much of a threat this all is. It feels like it's something out there in the world that is happening to other people, but it's not going to happen to me. Do you find that in your talks around the country that people feel like that it's not something that's going to happen to us?

Jeff Lanza: Well yeah, people they tend to think, well they're in denial. This is not going to happen to me. If you're in denial you know what happens, that's when it

happens to you because we don't take the steps necessary to keep ourselves safe.

These crimes are in epidemic proportions. The FBI has fought against crime epidemics for years. The answer to the crime epidemics, solving those crime epidemics in the past was you arrest people, you put them in jail, there's deterrents and incarceration, and so forth. We can't get at the people that are doing the crime epidemic that involves what you're talking about, that involves email account hijacking and bank account takeovers. Most of them are in foreign countries and Russia is not going to extradite those people that are doing that. They're not going to extradite the people responsible for the DNC hack. The only way to stay safe is to be careful where we click in these type of examples because the FBI is not going to be able to stop today's crime epidemic which involves exactly what you're talking about.

Bill Keen: We've talked on the program Steve, this seems just natural I think. This other thing has happened to about everybody where you start getting charges on your credit card from other states in places and you don't recognize them. You're able to call the credit card company, or heck, even the credit card companies now are so good that they'll ask you within minutes, "Is this real," and you say, "No," and they just cancel it, and you kind of go on. Is that considered identity theft, what is that considered?

Jeff Lanza: No, that's just credit card fraud. If someone gets your credit card number sometimes you never know how they got it. It could be a variety of different ways. They try to use your card for fraud. Sometimes the charges will go through, sometimes they'll be stopped by the credit card company. Sometimes you get a text message and say, "Is this you?" Even if this charge went through we're not going to have to pay the money. The credit card company will take it off our bill and they're going to eat the cost or the merchant will eat the cost, it's not going to be us. You get a new credit card in the mail, it's a little bit of a hassle.

Identity theft is different than that. Identity theft is where they open new accounts using your identity. They get a new credit card account using your name and Social Security number and you don't even know it's out there. You're not getting a text message. You're not getting a phone call that said, "Is this you?" The phone call is going to the criminal, if there is a phone call. Identity theft is when these accounts are opened in your name that you don't know about. We call it new account fraud. It doesn't involve a current credit card that you have. That's the problem, you don't even know it's happening. You don't even know it's out there.

Bill Keen: That makes sense. I have to mention this briefly Steve. I was reading Jeff's book a while back and you might recall one of our prior episodes I said when my credit card was hacked, or I guess my credit card was being used for fraudulent purchases I recognized after a couple days that I was better off. The fraudsters

were spending less than all the various people in my family that had a credit card. Remember?

Steve Sanduski: Yeah, I do.

Bill Keen: I did not copy that off Jeff Lanza, but I found it in his book here, in one of the intros to the chapter. Do you remember what is says here, I'm paging through it now Jeff.

Jeff Lanza: It's about a person, I won't say it was a man or a woman, a person had his credit cards stolen and being used for fraud. I said, "Did you report it to the police?" "No." "Did you report it to the credit card company?" "No." I said, "Why?" He says, "Because whoever stole this is spending less than my spouse."

Steve Sanduski: I guess it just goes to show that great comedians think alike, right?

Jeff Lanza: One of the things that as a general rule, if something doesn't make sense online then just don't click on it. In other words, if you're getting an email that doesn't look right, if you're getting something from someone who sent you a document to look at and you don't know this person, they wouldn't normally be sending you documents, then just don't click on it. Common sense goes a long way to preventing fraud. Then criminals always try to make it so we're using emotions to make decisions. There's going to be some kind of an emotional component in an email, something's happened to your credit card, your PayPal account has been breached, you want to make some money, you fill out this survey and get $15. All you have to do is click here and log in to your bank account. Now, if things don't make sense then don't click. Never let emotions overcome logic and common sense. There's almost always an emotional component.

To illustrate that point I have just a little story. It happened here in Kansas City when I had an agent. We had a mobster's phone tapped, a quarter tap on a mobster. His name was Tony. He gets a call from Joe. Now as we listen to the conversation here's how it goes, Tony says, "Joe, I'm glad you called." Joe says, "Why?" Tony says, "I have a problem. I think the FBI is tapping my phone." Joe goes, "What are you going to do about it?" Tony says, "Well I already got a solution to the problem. I got it figured out. I got a new phone number." Lacking any common sense Joe says, "Oh give you the number?" Tony gets a little common sense, he says, "I better not give the number over the phone. I'll meet you for lunch and I'll give it you then." Joe says, "Well I can't meet you for lunch." Tony says, "Okay, I'll give you the number over the phone right now, but I'll give it to you backwards." So he proceeded to give him the seven digits in reverse order. What did the FBI do? We got our best cryptologist on that right away.

Steve Sanduski: You probably had to use the enigma machine for that one.

Jeff Lanza: That's right, I was going to say it only took us six months to figure it out. I use that story for humor in my presentations, but also to illustrate that how important is common sense in everyday life. When it comes to scams it's almost always the case there's some emotional component where the criminals are trying to get us to use our emotions, the wrong part of our brain to make decisions. We got to watch out for that.

Steve Sanduski: You mentioned ID theft earlier. You hear these commercials for these companies that will protect you if your ID is stolen. How do those work and are those just insurance policies? What is the potential benefit of a service like that?

Jeff Lanza: You're talking about companies that monitor your credit reports. The most ubiquitous name in the industry is LifeLock, you hear that advertised a lot. It's not really an insurance policy. You hire LifeLock or many other companies like LifeLock, they will monitor your credit reports and if there's activity they let you know that it's happened. Let's say someone steals your identity. They try to get an account open in your name, get a loan in your name. A credit report is generated and LifeLock sees that's been generated, and they tell you that it's happened. Normally that notification occurs after the crime has happened. Not always, sometimes they notify you before or while it's happening and you have time to stop it. Most cases, it doesn't prevent the fraud from happening and there's no real insurance. We're not paying you back any money if you've lost money because it doesn't involve a loss of money as much as just time and hassle to get your life back together and to get this criminal out of your stuff. It's more they let you know it's happened so you can act sooner. For some people, that's a valuable resource and they also tell you what to do if it has happened and some people need that help as well. That's what those services are about.

Freezing your credit reports has a better effect because it locks it down. The crime never occurs to begin with.

Steve Sanduski: If you were to freeze your credit report what if you do have a legitimate need for a loan or something like that, do you just go in and say I need to unfreeze my credit report for a couple days here? How does that work?

Jeff Lanza: That's a great question. You need to unfreeze it or also it's referred to as lift your credit freeze. You can do that with a pin number. When you freeze your credit reports you get a pin number. Don't forget the pin number because you can't lift it without the pin number, so you keep that in a safe place then you lift it temporarily and then you freeze it again.

Bill Keen: When we store that pin number should we store it in the reverse order of the actual numbers?

Jeff Lanza: Yeah, only if it's seven digits and it has a phone number syntax to it.

Bill Keen: What about, real quick, for open accounts that you have? Most of us have some sort of revolving credit accounts, if you freeze your credit it doesn't affect those.

Jeff Lanza: Correct. It does not affect your current credit cards and other open accounts. They can still check your credit. They can still put information in on your payment history. It doesn't affect those. It's only new accounts that are being opened in your name.

Bill Keen: Okay, perfect.

Jeff Lanza: No one can get access to your credit reports except those companies you have these relationships with. There are some there exceptions as well.

Bill Keen: Okay, okay, good.

Steve Sanduski: How about we are out and about and we are on Wi-Fi and we decide, gosh, I want to see the value of my investment account. I log in to TD Ameritrade and I'm on the hotel Wi-Fi. Am I just totally exposing myself doing something like that?

Jeff Lanza: You potentially are. Open Wi-Fi networks are not secure and people need to be cognizant of that. You'll see the warning when you log into these sites there's usually a warning, a disclaimer page, that says, "Other people can see information here." You never want to use an open Wi-Fi to log in to your financial accounts, log into your other financial accounts like bank accounts and so forth. Even email accounts your credentials are potentially being exposed.

Then there's two ways to be safe in open Wi-Fi networks, not use them at all. Instead of using them if you have a recent model phone you can use the cellular function of your phone as a personal hotspot, so you go into the settings, you turn on hotspot, and that will create basically a Wi-Fi network for you using the cellular network on your phone, which is much more secure than a Wi-Fi network in a hotel, for instance. Or, you can get what's called a VPN, which is a virtual private network. They are as cheap as $3 a month, you go online, you download the software for that, and when your Wi-Fi initiates in your open Wi-Fi network you instead use the VPN which creates a secure and encrypted tunnel between you, your computer, and the site you're community with. So a VPN or your personal hot spot would be the best way to communicate that way.

Steve Sanduski: Bill, I think at your firm don't you have some type of security dome where you guys are logging into a different system, which is essentially protecting everything from the outside?

Bill Keen: For sure. We call it a VPN or our environment that no one here at the firm is allowed to do anything except through the secure environment. That's correct. Then of course our main custodian Charles Schwab has gone to great lengths to protect assets and accounts. Then we have a protocol here at the firm as well

that no one takes any instructions over email ever. We have to talk to or see the person before any money moves or leaves any of these accounts that we manage, period. There's no exceptions to that.

Steve Sanduski: Jeff, what about social media? All of us are on social media, what are some tips that you have for us to make sure that we don't do something dumb in social media?

Jeff Lanza: Well the main thing I would say to people is just understand that nothing's private. When you start putting stuff on social media privacy is gone. I think people know that now and they know based on what's happened with Facebook and other accounts that once you put stuff out there it can never be protected. What I tell people is just keep your social media accounts private to the extent that only people that you approve can see your information. The whole world can't see that you're on vacation in Hawaii and you're away from your home, for instance, very simple thing, only your friends can see that. That would be a way to limit who has that information as well.

What I tell people is on social media, Linkedin, Facebook, Twitter is just watch how you log in. Again, never log in through a link because the hackers are out there trying to steal our social media accounts as well, get access to those, and get personal information from those accounts. Be careful what you put out there. Keep your information as private as possible. Just know that anything you do put out there could get in the hands of somebody who could use it for these purposes of further fraud.

Steve Sanduski: You mentioned the log in. I'll go to a website and it will say, "You can log in using Linkedin," or, "You can log in using Google," or, "You can log in using Facebook." Should we do that? Should we log in to an unrelated site using the credentials of say Facebook or does that expose us to further issues?

Jeff Lanza: No, actually it's better because you're not typing in your password on these sites. You're already logged into Facebook on your computer, for instance, and you can log in using those credentials. That limits the amount of information you're putting into these websites. It negates the idea that you have to create another user name and password in. In fact, I have a section about that in my book. When you get a chance to log in through a social media site you can do that and it doesn't create any more risk to you.

Steve Sanduski: You mentioned your book. Why don't we talk about that for a minute.

Jeff Lanza: Sure.

Steve Sanduski: You do have this new book called "Cyber Crime: How to Stay Safe from Online Fraud and Identity Theft." Tell us a little bit about the impetus for putting that book together.

Jeff Lanza: Well I've been giving speeches of a long time on the topics of identity theft and cyber crime. I present a certain number of topics on these presentations and then people ask questions. Judging by the amount of information that I present and what people ask I realize that maybe I should put this all in a book because people want to take it home. They want to have something to read. They want to stay educated on these topics.

After the Equifax breech that occurred I thought I really needed to put something together. My book actually was ready to go when Equifax happened. In fact, my book was published on the day of the Equifax breach, September 7th, 2017. It came out on that day.

It's available on my website. I don't sell it in bookstores. I sell at my events and I sell it on my website. It contains information about how to stay safe from identity theft and how to stay safe from cyber crime, email account hijacking, bank account takeovers. There's a section on passwords and how to create strong passwords or passphrases and just to stay safe from criminals who are guessing our passwords through very strong programs they can use to do that. Those are just a sample of things, much, much more in that.

Bill Keen: It's a great book Steve. I've read through it multiple times and have garnered so much information that you don't hear bantered about typically in your typical blog post or brief things you might hear online. Highly recommend it.

Steve Sanduski: Well we'll definitely link to that on the show notes at keenonretirement.com. If people want to go direct to it I believe the website Jeff is thelanzagroup.com, that's T-H-E L-A-N-Z-A Group.com. You can find the information there on the book.

Anything since you published the book that's come out that you think, gosh, if I could add another chapter to the book this is what I would talk about today? I know it's still a new book.

Jeff Lanza: Yeah. Probably if I was going to add more information to it, it would be a little bit more about the government changing it's guidance on password. We don't use passwords anymore. Now the government is calling it pass phrases. We're trying to change people's perception of passwords being long, and complex, and upper and lower case, and a number and a symbol. That forces people not to use different passwords for all these different sites that they use online. It forces people maybe to write them down and keep them on a piece of paper at their desk. These are not secure as well. The government is trying to move to something a little more simple, pass phrases, putting together words, taking out spaces, and using that. Making it long enough to be strong and then also ... I do have all that in my book, but what I talk about since then is the way to store passwords or pass phrases.

If you have an iPhone you can actually secure notes on an iPhone. Most people who have iPhones may have used a note function. You put something in Notes so you remember it later. There's a way to store those notes securely by putting a password on a note. You can put all your secure documents, secure information, pass phrases in that particular note, assign a pass phrase to that note, and then no one can get access to that note, but you have it with you all the time on your phone. You do on an Android too with an app.

Steve Sanduski: Along those lines, I actually use an app to store all my passwords. Is that a good idea or a bad idea? Obviously I've got a strong password to get into that master password manager, but then when I go to a website as long as I'm logged into that password manager it will basically pre-fill in my user name and password. Is that a good idea, bad idea?

Jeff Lanza: It's a good idea. In fact, it's a great idea. I recommend everyone get some sort of password manager or use that note app I just talked about in a secure way via Apple or Android devices. Absolutely, they've proven to be secure, reliable, and they help us manage all the passwords that we have in our lives.

Bill Keen: Jeff, someone told me at one point that Apple phones are difficult for fraudsters to download things on, is that true or-

Jeff Lanza: Yes.

Bill Keen: ... that doesn't mean we're exempt from any of this happening on an Apple phone does it?

Jeff Lanza: The iOS software is very secure and the apple phones themselves are very, very secure. They're pretty much locked down. Any time I'm testing out an email that I think contains malware and I want to see where it sends me so I can maybe use it as an example in my presentation I will never open that up on my computer, which is a Microsoft computer. I'll open up the email on my iPhone and click anywhere I want. I am almost certain my phone's not going to be infected with malware. I think Apple's really locked down when it comes to that and Android devices as well. The only difference with an Android is that you can download apps in other places besides Google Play. Those could be dangerous or risky, so I recommend if you have an Android you only download the apps from the Google Play store, from nowhere else. Apple only lets you download apps from their store, which is highly vetted as well.

Bill Keen: Okay, that helps.

We talked a little bit before we talked about how folks will use phone numbers or see emails, things that they've recognized in the past and that provides them a false sense of security. I wanted to ask you if you could tell us the story about your time that you were doing an investigation, on scene on a bust that had happened. Would you be willing to share that with our audience?

Jeff Lanza: Sure, I could share that in a brief was.

Bill Keen: Steve, I think you'll like this buddy.

Jeff Lanza: One of my first cases I ever worked on here was a case involving a bookie. This was back in 1988 when I first became an agent. This bookie was taking bets over the phone, over a landline phone. We had a tap on his phone. There was an agent listening to his conversations. It was a court ordered wiretap, time to bust the bookie based on the information that we got. We go to the bookie's house, there's an agent in charge of the case, I'm brand new in the office. He's interviewing the bookie. I'm at the bookie's desk. It's a Sunday morning. It's September. Baseball is in season, football is in season. I'm at a bookie's desk. What might happen next Steve do you think under those circumstances? The phone rings. I'm new in the office, so I don't know should I answer it or not. I'm a brand-new agent, I ask the agent in charge of the case, I go, "What do you want me to do with the phone?" He goes, "Pick it up." I answer the phone.

Now before I tell you what happened next I got to back up a little bit. I grew up in Connecticut. My dad owned a business, it was a small convenience store. These guys used to come into my dad's store all the time and bet on games themselves, but they'd hang out in my dad's store and talk about what games they're going to bet on that day with their bookie. I'm a teenager, I don't know anything about gambling, but I hear these guys talking about the lines on the game, I'm taking Detroit minus 130, I'm taking the over on Cincinnati. I hear all the lingo of gambling. I learned all about gambling that way. That's my story and I'm sticking to it.

Fast forward 15 years, now I'm an FBI agent. I'm at the bookie's desk, the phone rings. I got my gun, I got my badge, we got our FBI ray jacket, big jacket, blue jacket, FBI yellow letters on the back. We got the search warrant, everything's official. Guy on the other line says, "Hey, who's this?" I tell him my real name. We're only busting the bookie, not the betters. So I say, "Jeff." He doesn't say, "Jeff who?" He doesn't say, "Jeff, where's my bookie." He says, "Hey Jeff, what's the line on the Chief's today?" Well I knew how to read the lines, I remember from my dad's store. I figured why not tell the guy. So I tell him, "Chiefs are minus three and a half." He goes, "Give me $50 on the Chiefs." I go, "You got it." So I take down his bet. I hang up the phone. My hand is still-

Steve Sanduski: And you're feeling good right now.

Jeff Lanza: My hand is still on the receive. It rings again, another caller. "Jeff, what's the over on the Vikings." I knew about over/unders, total point score in the game. "44-45, how much you want?" "Give my $75 on the over." I go, "You got it."

It's approaching noon central time. The phone's ringing off the hook. Guy calls up he goes, "I want to do a two-team bet." We call that a parley bet. You do two team parleys or three team parleys. You got to win them all, if you do, you get

odds on your wager. He forgot what the odds were on a two-team parley, so he asks me. He goes, "Hey Jeff, I want to do a two-team parley. What are the odds on the that?" I remember from my dad's store, two team parley pays 12 to 15, who doesn't know that? So he's goes, "All right, give $50, Yankees/Jets two team parley." He goes, "Pays $120 to win." I go, "You got it."

That goes on for about an hour. By the way, another guy calls up and he goes, "Jeff, wait a minute, wait a minute, are you still going to pay me if I win?" I played along, what was I going to do, right? I told him, "Oh yeah, don't worry. We'll pay you." He gives me his first name, last name, address, he spells it out one letter at a time to make sure he had it just right so he'd be paid on Tuesday. "So it's Mike Smith, S-M-I-T-H, 333 Maple, M-A-P-L-E, Kansas City, Missouri, 64105. You're still coming by on Tuesday, right?" I go, "Oh yeah Mike, we'll be by. Don't you worry about that."

Finally, after an hour of that a smart guy calls up. We should all be this careful. He goes, "Wait a second, wait, wait, Jeff, Jeff, Jeff who?" I tell him the truth, "I'm undercover. We're just busting the bookie." I tell him, "Jeff with the FBI." I expect I'm going to hear click, that's not what I heard. He didn't hang up. He starts cracking up. "Jeff with the FBI, that's a good one. He answered the bookie's phone, that's really funny. I love that. I love that Jeff with the FBI. Hey Jeff with the FBI, give me $50 on the Chiefs will ya?"

Steve Sanduski: You sure you don't want that a two-team parley 12-5 odds.

Jeff Lanza: That was my day as an FBI bookie, by the way.

Steve Sanduski: That's awesome.

Bill Keen: The point too, and a point, which is an awesome story, but the point is they were familiar when they called the number ... Is that right? That's the-

Jeff Lanza: Right.

Bill Keen: ... point that you were making?

Jeff Lanza: The point is, know who you're talking to. Know who you're giving information to on the phone. You'd be surprised, it's not just computers. We have people, probably clients of yours Bill that get calls from people all the time, "This is the IRS," or, "This is your bank, please send us money because otherwise you're going to be arrested," or, "Your bank account is going to be closed." You never give information, never provide access to your accounts, or money to anyone unless you've verified who you're talking to. That's the whole point of that story really.

Bill Keen: Yes.

Steve Sanduski: Excellent. Well Bill, why don't you take us home here?

Bill Keen: Well we really felt like it was important to reach out to Jeff. You might recall that when the Equifax breach came out that we did a podcast on cyber security and tried to do our best in bringing information to the table. But I mentioned Jeff by name. I mentioned Jeff Lanza because I read some of his stuff and I was basically bringing that information to the podcast as best I could then. Since then, because of the way things have played out and continue to play out. We reached out to Jeff and said, "Is there any possible way you could come and be on our podcast personally?" I didn't know if we could pull it off and we were able to. I was very grateful. It's quite a privilege to have him here in the studio.

Jeff is also doing a live event for us, which we can give more information on if anybody would like to attend that feel free to send me an email through the website. Super grateful Jeff to have you.

Jeff Lanza: You're welcome.

Bill Keen: It is a true privilege to have him here in the studio with us and on the show Steve.

Steve Sanduski: All right, well thank you Bill. Thank you, Jeff.

Jeff Lanza: You're welcome.

Steve Sanduski: If you want more information about what Jeff is doing you can go to thelanzagroup.com. The also we'll have all the notes here at keenonretirement.com.

Gentlemen, thank you and we'll look forward to the next episode.

Bill Keen: All right, thank you Steve.