THE Patti Brennan SHOW

Ep89: Am I At Risk for Having My Identity Stolen?

January 28, 2022

PATTI BRENNAN: Hi, everybody. Welcome to the "Patti Brennan Show". Whether you have $20 or $20 million, this show is for those of you who want to protect, grow, and use your assets to live your very best lives. Today, we're going to be talking about how to preserve them.

In other words, preserve them from fraud and keep them away from the clutches of cybercriminals. We were talking about this earlier, and it just seems like it's happening more and more, and you're hearing about big companies who are having to pay these huge ransoms.

I think that it's unfortunate. Is it because of COVID? Is it because these white-collar criminals are thinking up new and different ways of getting us? Maybe, maybe not. Today, what I'd like to do is bring to your attention some of the more popular ones that are out there now, and then talk about what you can do to make sure it doesn't happen to you.

Number one, what's unfortunately happening, because of COVID 19, there are people who are getting phone calls from government agencies claiming to be providing relief payments. All they really need is your Social Security Number and your date of birth. You're going to get this wonderful payment.

Don't fall for it. They're not calling people on the phone. If you are eligible for one of those payments, you're going to get a beautifully written letter from President Biden in the mail, and then the payment will follow. Don't fall for that.

Number two, the Social Security Administration, same thing. It could be a call saying that your Social Security payments are going to stop, or they're going to claim something or other, and then try and get that information from you.

Same thing for Medicare. They're not going to pay your Medicare benefits unless you give them your Social Security Number, your date of birth, your address. Remember, they're not going to ask for this stuff upfront.

They're going to say that we understand that you've had a recent illness, and they're getting this information...God only knows how they're getting it, but they are. Keep in

mind, guys, your email address is the easiest thing to hack.

There is no privacy when it comes to your email address anymore and your emails. Just be aware of that before you send somebody an email talking about the surgery that you just had, because a hacker could read that and have that information when they call you on the phone.

Again, you've just got to assume the worst when it comes to these tools. Same thing with social media. Everybody knows that at this point, but I always like to bring it up again. Whatever you publish on Facebook or any of the social media sites, these cybercriminals are gathering all that information and gathering that data to, again, get rapport, reach out to you.

Whether it be by phone or by email, they're just going to do it. Again, the emails are really scary, because for example, we all know that you can get an email. It could be an email from yourself, and you're like, "What is this all about?" because they have your email address.

It's just to get your attention and ask you for personal information. There's a new scam out there. We all know about phishing. Phishing is when you're on an email, and it tells you that you have a package that they're trying to deliver.

If you just click on this link, you can see where the package is and why it can't be delivered. In that case, and in all of these cases, please don't ever click on a link in an email. I'm just saying, "Don't ever do." Never, never, never.

It's not even right-click on the email address from which it's coming and see and make sure it's legit. Even that's hard to figure out. If you get one of these emails, go out of your Outlook or wherever you do your Gmail, what have you.

Go on the URL. Go on the site itself, and tap in, whatever it is, the information that you give you, and see whether or not there actually even is a package. Another one that I've talked to you about before is Amazon.

Amazon, these fraudsters are calling people, pretending they are from Amazon security. They're saying things like, "We have noticed some activity on your Amazon account. Did you make the following charges? Did you charge $119.36 at Target? Did you do this? Did you do that?"

Of course, they're bogus. What do they do next? Well, the person who's on the other line says, "OK, we will remove these charges from your Amazon account. Will you help us catch these people? Will you help us?" making you feel like the hero.

You're the hero. You're going to now prevent this from happening to other people, because, "We were lucky. We caught this for you, but we're not able to catch all of these people, so can you help us catch them?"

We know of a situation where someone was taken by over $100,000. I won't go into it today because of how they did this scam. The bottom line is, guys, don't ever – and I mean ever, just like clicking on a link – don't ever wire money or get gift cards and send them to some random places based on something that somebody told you over the phone.

Not even 9 times out of 10, not even 99 times out of 100. I'm telling you all, it's probably fraud. Don't do it, OK? We talked about that. Here's another one. We know that passwords and usernames are now easily hacked.

In our quarterly letter, I was talking about this issue, and there's a chart here that I'm holding. It basically tells you the amount of time it takes for a hacker to get your password. If you have 10 numbers in your password, 10 characters, they can instantly hack it.

It's not a big deal. These people are unbelievable. If you have a lowercase letter and 10 numbers, it takes 58 minutes to figure out what your password is. If you really want to protect...This chart is so cool, I must tell you, because it's got the what's instant, versus what's in the yellow line, versus what's green.

If you really want to make your passwords hacker-proof, if you have 18 characters, with upper and lowercase letters, it takes 110 years for a hacker to figure it out. The bottom line is, the more characters you have to your passwords...

Don't forget those exclamation points and those starts, because you can use those as well. It just makes it more and more difficult for them to figure it out and steal your money. This spear-phishing thing – we know about phishing, but – what's spear phishing?

Spear phishing is where they've figure out one of your usernames and passwords. They send you an email, and they say, "Hey, I've got your username and your password for Amazon. It is blank and blank," and sure enough, it's your username and your password. They've figured it out.

What they're doing is they're saying, "And, by the way, this is only one of the accounts that we have, so you need to contact us immediately." It's basically another ransom thing, "Because we have all of your passwords and your usernames." That's spear phishing.

Chances are, they don't really have all of your usernames and passwords. Hopefully, you're not using the same password for multiple sites. Again, don't give in to these people. Just change that Amazon, in this case. Change your username and your password.

By the way, think about putting 18 letters to it, or 18 characters to it, to make it really bulletproof. Speaking of which, we've talked about the problems. What are some solutions? Again, get better passwords. Really make it difficult.

A lot of these sites will offer two-factor authentication. Do it. Don't even think about it. Do it. What is two-factor? Basically, when you put in your username and your password, then they're going to send a code to your cellphone.

You have to have your cellphone, or the hacker has to have the cellphone, right on them to put the code in to get into that. Two-factor authentication is also a great way to defend your personal information and prevent identity theft.

Think about also these password managers, LastPass, and a number of them, because a lot of us have a lot of sites that we go into. I can't remember all of these passwords. These password managers will remember them for you, so you only have to remember one.

Again, for that password manager, make it really long and really difficult to figure out. Somehow, someway, again, because you don't know if something's going to happen to you, you've got to give that to somebody who you can trust who will also know what that username and password is to the password manager.

Last, but not least, to protect yourself, and protect what you've worked for, think about freezing your credit. It sounds like a drastic step. It's not as bad or difficult to unfreeze it as it used to be. Remember, we had the Experian hack many years ago.

325 million Americans – myself included – our Social Security Numbers are now in the dark web. If you recall that, hopefully, you went online and figure out whether or not your Social Security Number was one of them.

You need to be really careful. Be extra diligent. I would say, if yours was one of them, and even if it wasn't, just literally think about freezing your credit with the three credit agencies. Again, there are programs out there, LifeLock being one of them, Experian being another.

There are different programs out there that will help you monitor your credit, help you to freeze your credit, even provide insurance, in the event that you are a victim of identity theft. I hope you found that helpful.

I'm going to continue to do these quick broadcasts to answer questions that you might have, and this probably won't be the last time we talk about this subject, because we're always hearing about the latest and greatest scheme where people's money and they were taken.

I just want to keep you aware of what's out there, and again, feel free. Go to my website at keyfinancialinc.com. Ask those questions, because that's what makes these vignettes powerful. These are questions that you all have asked us.

Whether it be through the website, in person, or even calling us on the phone, that's what we're here for. Thank you so much for giving us these ideas and this content, and thank you so much for tuning in today. I hope you have a great day. I'm Patti Brennan, Key Financial.