KEEN ON
RETIREMENT

4 Important Cybersecurity Lessons to Protect Your Info—And Your Money

Welcome to Keen on Retirement
With Bill Keen and Steve Sanduski

Steve Sanduski: We are back with another episode of Keen on Retirement. I'm your co-host Steve Sanduski and I am here with my two partners in crime today, Bill Keen and Matt Wilson.

Gentlemen, we've got another great show lined up today.

Bill Keen: Yes, we do, Steve. It's going to be an interesting episode. It's too bad that we have to discuss some of the issues we're going to be talking about today, but I think it's in our listeners' best interest to go there, and we're grateful to have Matt here in the studio with us. We missed him last week, didn't we?

Steve Sanduski: We did, we did, yeah. And we teased today's episode, when I talked about partner in crime, so that's a little hint on what's gonna happen here today.

Matt Wilson: Yeah, October is National Cybersecurity Awareness Month according to The Department of Homeland Security.

Bill Keen: I thought that-

Matt Wilson: Hopefully, I'm not looking at a fake website.

Bill Keen: I thought that came from Hallmark.

Matt Wilson: Yeah, that's a Kansas City company here, Steve. You think they have cards now for this? They might.

Bill Keen: We can send them over a new idea.

Matt Wilson: Well, they're probably online cards now as you might think, so.

Bill Keen: Mm-hmm.

Matt Wilson: All I know is if you get a paper card, it's like 5 or 6 bucks. They're not inexpensive anymore.

Bill Keen: And, well, they're special now. They've gone back to being special receiving those actual cards. Well, Steve, thank you for allowing us to go where we're going today with this episode, and we do not want to be alarmists here on the Keen on Retirement podcast, but we do want to be realists.

And with the recent Equifax breach, we just thought it would make sense to have an episode dedicated solely to this. We mention it in blogs, and we've mentioned cybersecurity in the past in an episode probably a year ago or so, but we thought today, after all the questions we've been receiving in the firm, that we would really go deeper with it and share with our listeners what we're hearing, what the questions are, with the research that we're doing, with our providers and our consultants and our custodian, Charles Schwab, what they're doing, what they're recommending.

We even have an FBI agent here in Kansas City who's retired now but had specialized in this area that we have information on as well. In fact, we'd like to get him on our program at some point in the future, maybe even have him come as a speaker.

But today we wanted to dedicate the show to this because, frankly, some of this is shocking, and the questions are gonna be what do we do about it, really. It's always the question. What do we do about it?

Matt Wilson: Yeah. You're right. What do we do about it? And just understanding what the problem is and, man, they're, it is so easy to be fooled by these online scammers that can get your email address. They can get your social security number, and next thing you know, they're into your bank accounts, they can take out loans in your name. And all this can happen in a flash. And, yeah, so it's gonna be, I think this will be a very timely and helpful episode to really help people protect themselves against some of this fraud that's happening out there.

Bill Keen: Yeah, do you remember a blog recently about how my daughter had her bank account drained, Steve, and had things ordered online and sent to our house? Remember that complicated scheme we wrote about? Maybe we can link back to that episode in the show notes, but I was just sitting here thinking, do I know of anybody that has had their identity stolen because it becomes real when it's your family or your friends or your acquaintances, and, you know, in my mind, I guess that's a little mini example of having your identity stolen, isn't it?

Matt Wilson: Yeah, definitely, and I'm sure we all know someone, if not ourselves, that have been breached like that. We know someone who has. I've got a friend of mine

who told me a story about how somebody ordered five iPhones on his account. He got a phone call from, I guess it was Verizon or somebody and they were asking about it, and he's like, I have no idea what you're talking about.

And so somehow they ordered five iPhones on his account, so just a weird deal. Of course, it took him hours and hours of runaround to get it squared away. But, yeah, it's not only the financial implication here, but it's also the time that if you do get a breach, it can take hours and hours and hours to get things squared away.

Bill Keen: That's right and you know with all this talk of Equifax being the most recent one, and probably a shocking one because it's such irony that they're a company that is supposed to be coordinating and calculating our credit, I guess, but the other thing about this one is that no one, you know, no one signed up for Equifax. No one opted in and gave them their data. They have all our data. We didn't have a choice. But I did have a list of documents here because Equifax, yes, the last number I've seen is 143 million people compromised.

I just saw something come out recently that 10 million of those actually included driver's license information, for what that's worth, but I have 12 pages of data breaches that have occurred, you know, I would call it in the last five to seven years.

Yahoo. Remember Yahoo? And I think Yahoo didn't announce theirs until what, years later? Didn't they say, hey guys and gals, we had three, did I see three billion? I'm seeing three billion as a number of people that was breached through Yahoo. Is it possible that they had three billion?

Matt Wilson: I don't know. It sounds like a lot of fake accounts.

Bill Keen: It must be. That's almost half the world populations.

Matt Wilson: Yeah.

Bill Keen: Yeah, so they announced that three years after they announced it. They said they figured it out or something. I'm looking at, let's see here, some more Zappos in 2012, 24 million people compromised. I'm seeing the National Guard of the United States, 131 million. UPS - they don't have a number on that - 51 locations, they say here. Starbucks, 97,000 people. I mean, so I've got 12 pages of this, so my question would be, if you're hacked, which one of these, which one of these caused your problem? I guess it really doesn't matter which one caused your problem.

The question is how do you fix it, and how do you avoid it? JPMorgan, 76 million people compromised in 2014. The list truly goes on here so, one last thing. I feel like I'm dominating you two so I'll step back here in a moment. I'll stand down. But I was doing some research on this, and this is again another irony.

Someone has made a fake Equifax site and then Equifax linked to it. So we had folks calling us, didn't we, Matt, saying, hey, Equifax is now giving us the opportunity to log, to click on a link to have credit monitoring services.

Matt Wilson: Yeah.

Bill Keen: But they just compromised us once, so now we're gonna click in there and the first thing it asks you for is your social security number.

Matt Wilson: Yeah, yeah.

Bill Keen: So, we know people create fake versions of big companies' websites all the time, usually for this, phishing purposes, but usually the big companies don't link to them on accident, but actually Equifax did.

So I'd like to talk today about some of the things that you can do. Maybe define some of these things that you always hear about and then what are the action items that we should be taking.

Steve Sanduski: So there's definitely a few things that all of us can do, some simple precautions that we can take to avoid. Now, we've got the Equifax situation. There probably wasn't a whole lot we could do because that was the company that messed up there, but things that are in our control are things like our email. And we can implement what's called a two-step verification or two-factor verification.

And this is something that you have to be proactive in, so depending on what type of email system you're using, you, it's a setting where you would actually have to flip a switch in your settings area for two-factor identification, so essentially it means if someone is trying to change your password, something like that, then they will have to send you another email to your predesignated email address and you have to approve that, so basically it alerts you that something is being changed. It just doesn't automatically happen. And this is also typically in place for different apps that you might use, whether it's an Amazon or Google or things like that, Apple. Typically, they do offer the ability with this two-step verification, so definitely encourage folks who are listening to check the different software that you use and make sure you have this two-factor identification in place.

Bill Keen: You know, we've got the new iPhone coming out that says it'll just use your face, so I guess that's about as secure as you can get.

Steve Sanduski: Well, it is. It may not be as convenient for some people, and that definitely takes some time holding up the camera in front of you and taking a picture and everything so, yeah, there's definitely different ways that big companies are experimenting with different ways to unlock your phone and we'll see what wins out.

Bill Keen: Yeah. And you could see with the advent of so much stuff going mobile now and you've got iPads, iPhones, other types of tablets and similar devices that, yeah, maybe passwords ultimately become a thing of the past, and we've got other ways to unlock our accounts and identify ourselves.

Steve Sanduski: Yeah, yeah, definitely. Another thing to think about here is clicking on a hyperlink in an email. So this what they call phishing and that's not spelled with an "f". It's spelled with a p-h-i-s-h-i-n-g. So you'll get an email. It'll look like it's coming from a legitimate source and there'll be a link in there that looks official and you click on it and, boom. And things just start to explode from there and I've seen some numbers that say as high as 91% of cyber-attacks are the result of data breaches that begin with one of these phishing type emails, so if you have any concern that your email looks suspicious, or there's a, it looks a little bit funny or something's a little bit off, then don't click on that thing.

And sometimes you can also tell if you can look at the actual URL address, the web address, in, you know, one of the, if you can see that, it might look like it's coming from Amazon.com but actually it's Amazon, you know, 123.com, or they've got something that looks like Amazon.com in the email address but it's not actually Amazon. So with a little extra precaution, usually, you can figure those out and not click on them.

Bill Keen: In most cases, you hover over the link and it'll show you what you're about to click on. So let me define phishing.

Phishing is cybercriminals pretend to be a trustworthy source in order to acquire sensitive personal information such as user name, passwords, social security numbers and credit card details. We do get calls from time to time at the firm here where someone will say, we've received an email from, typically, it's our custodian, Schwab, asking for information or telling them an account has been locked. And it is never the case that that was a legitimate email.

I think if the scammers and the phishers, if you will, send every single person a Bank of America one, you know, I get, you get Bank of America ones, Wells Fargo ones, JPMorgan ones. They can send out basically four of the big banks and you're going to have one of those accounts. And you're gonna think, hey, wait, that is my, I do have an account with that institution.

A big one I've been seeing lately is PayPal. Have you all seen the PayPal one come through? I don't have a PayPal account, but it still gets my attention. I'm like, wait a second. Do I have a PayPal account? You know?

But they're simply trying to get you to bite on that and enter some data and give them some information. The other thing that can happen is when you click on one of those phishing emails is that it installs something called malware.

Malware is malicious software that's created to damage or disable computers, steal data or gain unauthorized access to your networks. And those are things like viruses, worms, Trojan horses, ransomware, spyware, all of those different things that come inside your computer and seriously are able to monitor and track everything you're doing.

Steve Sanduski: Well, I thought malware was like trendy clothing.

Bill Keen: See? I am out of the loop, Steve. All I have is suits and tennis shoes and running clothes. I don't have anything in the middle. My wife's often on me on that though. She tries to get me to buy the clothes that are in the middle, you know, so trendy clothes.

Steve Sanduski: There you go.

Matt Wilson: Yeah. You know, what they recommend is if you do get any emails from anything that is associated, maybe you do have an account with one of those major banks or financial institutions and you get an email from them, to never click on those links. You know, you just go direct to the website, login or, you know, call them directly and you can confirm exactly what they're needing. If they're asking you to log in and, you know, potentially, you know, you lose your credentials to some fraudster who has set you up in these, you know, phishing type scams.

Steve Sanduski: That's right.

Bill Keen: Well, another one that we need to keep in mind here is poor password practices. Now, this one's easy, where you think, gosh, you know, I'm always forgetting my password so I'm just gonna put in something that I can easily remember, like 12345678. Or 987654, or abc123, you know, something like that. So what happens is these sophisticated scammers, they have software that will simply try millions of different combinations of potential passwords that people might use.

It could be your last name plus a number. I mean, something like that, that a lot of people use, and they've got systems that will just blast at it until they find a password that works. They crack it and, boom, they drain you.

Steve Sanduski: Mm-hmm, mm-hmm. Yeah, what we, yeah, recommend individuals do on their passwords is at least 8 to 12 characters. You want to have both upper and lower case characters in there and, in addition to, you know, that, some sort of dollar sign, pound sign, percent sign, you know, one of those kind of unique identifiers in there and really try to randomize it.

Now, the hard part is remembering what those are and, you know, you think about it, okay, so then what do you do? Do you write it down somewhere, which now that's just open for someone else to find it. So, you know you've got

to be thoughtful on some of this stuff. Some people tell us they save them on their computer and it's like, well, that is okay I guess until you get hacked and they steal all of your passwords.

Bill Keen: Matt, do you have, you and I both have used Jeff Lanza's information. It's a well-known, well respected FBI agent, retired.

Matt Wilson: Yeah.

Bill Keen: We both reviewed his information and stay up to date on what he's advising folks. Do you recall the websites that he mentioned in his material, the one he even uses for his passwords?

Matt Wilson: Yeah, what he said is that he uses a, what's called a password manager, so it is a software program that he keeps on his computer, and, so there's one password to login to that and that's all he has to remember and then it saves all of his other passwords in this password manager and the name of that program was Keeper. And he mentioned there's an annual fee every year to keep the program on your computer and then it reminds you, too. Those types of software programs prompt you to update your passwords and change them because that's another recommendation is change them every three months, too, so that you don't have the same password always in there in case, you know, you do get it compromised. You're always changing it.

Bill Keen: That's right.

Steve Sanduski: And I use one of those password managers as well. I use one called LastPass. And it seems to work reasonably well. So I have this one master password to get into LastPass and then it stores all my usernames and passwords for the different sites that I go to.

Bill Keen: What he said is those are held on a secure server and it's an encrypted server, so if someone ever hacked those, they actually wouldn't be able to get into the data because the data's all encrypted. So, you know, and he's an expert in the cybersecurity field and that's what he said he uses, so I feel pretty confident in that process.

Steve Sanduski: Now, Bill and Matt, what are some of the precautions that you take there at Keen Wealth Advisor to secure your clients' information?

Bill Keen: We have automatic password resets on our systems here, so we're prompted to change those over time, you know, for our own, personal logins for all the team members here. But then, in addition to that, we have a lot of communications with clients over email and if we ever receive a request for any distributions via email, we have a policy in place here that we will call to confirm any email request and so that's something we always tell clients as, you know, as they're

signing on and setting up these distribution accounts. If they ever email us, we do need to speak to them before we're going to process that.

And most of them are appreciative of that. I mean, we don't get any complaints, considering the cybersecurity and the potential ramifications, if someone did get hacked and, you know, asked us to wire money and we didn't have that policy in place.

Steve Sanduski: One of the things that can happen is your email account is taken over. People are, the fraudsters are monitoring your activities, your times of day, the things you're doing, it doesn't take long to figure out how you communicate. And they literally can send an email to your financial institution requesting a wire transfer. So that's, again, we will not move anything without talking to somebody specifically. And we also look at the accounts, our accounts, every single day, don't we, Matt? The money flows in and out of every single account that we have here at the firm that we oversee.

Matt Wilson: That's right. We get notifications of any client initiated requests on deposits or withdrawals. And we monitor all of them.

Bill Keen: That's right.

Steve Sanduski: So what are some other things, guys, that our clients here can do? Now one of the things I know that's important is, obviously, credit card fraud can be a big deal. And I know with the credit card company that I use, if there is what they think is a suspicious transaction, it gets flagged and then I immediately get an email. And usually the way it happens is I'm trying to make a purchase on my credit card and it gets turned down. I'm like, what? What's going on here? And then, of course, I check my email. It says, "Would you please verify this purchase here?" And then I can click. It'll say if everything's okay, click okay. If it's not okay, then call us immediately.

And so, my company's doing a pretty good job of flagging those. And it's not so frequent that it's annoying, but it's frequent enough that I know that their technology and their algorithms are paying attention. So it's important, A, hopefully you've got a good credit card company, and then, B, when you do get your statements, make sure that you're checking those right away to see if there's any transactions on there that don't look good.

Matt Wilson: Credit card statements, any of your financial accounts, too, just always be monitoring those, because, yes, little things could slip through the cracks and you may miss it, especially nowadays where so many transactions are via credit card and debit cards. You know, hopefully, you're not doing too many debit card transactions just because we've talked about the issues with that, but with so many of those types of transactions, you know, it can be kind of a pain. But it's in your best interest to be monitoring that all the time.

Steve Sanduski: And we've talked about these credit monitoring services, haven't we, Matt, where, yes, it's fine they see something, but it is always after the fact.

Matt Wilson: Yeah, they'll monitor it and they'll warn you of suspicious activity or if someone opened up a fraudulent account in your name. They'll just tell you about it and then help you unwind that but they're not necessarily going to stop it from happening. And so, you know, because of this whole Equifax situation, people have asked us a lot, okay, now what do we do, and really the most, yeah, what we would say DEFCON 5 situation is you put a freeze on your credit. And so you're essentially locking everything down, no one can do anything in your name with your credit.

And there's three credit bureaus and you have to do that at each one of them. There's a process to turn it off. And there's a process to turn it back on. And there's a fee to do that. You know, it depends on the state.

Bill Keen: Ten dollars or so.

Matt Wilson: Yeah. It's not a lot, but it is something to be aware of. And that is, if you're not planning on doing anything, you know, with any credit accounts, opening accounts or applying for any credit, then that is a solution to prevent anything from happening.

Steve Sanduski: What, just a quick thing. Less than 1% of the U.S. public has actually done credit freezes. I just saw a number come out this morning. So we're recommending this and now the big agencies are recommending that as an option but less than 1% of the people have actually done it. But it's still something that, and I have not done it. Have you done it, Matt? Did you freeze your credit?

Matt Wilson: I have not. And you know, we hear about all these credit, you know, or data breaches from email accounts and passwords and user names and all kinds of different things, but you know, outside of fraudulent transactions on credit cards, we very rarely come across anybody who's had anything significant happen to them, whether, with like an ID, identity theft type situation. Most of them are, yeah, they were able to hack a credit card account and order stuff illegally and then the credit card company takes over and wipes it all out. So, I think most people aren't prompted to go that route because they don't feel like the risk of something significant happening is that high. And, you know, I would agree with that. It just, when it does happen, it is a very painful and time consuming process as Steve has mentioned.

Steve Sanduski: That's right. And I have one case and, Matt, you might recall that we had a client who filed their taxes about five years ago and they, where they had a nice return coming back and the IRS let them know that they had already received their return.

Matt Wilson: Yeah, they couldn't file their tax return because it was already filed.

Steve Sanduski: Yeah. Someone had already filed it.

Matt Wilson: Yeah.

Steve Sanduski: It took them several years to unwind that, so that's a case where there was real money tied up for years in that situation.

Matt Wilson: Yeah, and if something like that does happen, you know, the IRS does have a process where you can go online and then apply for a PIN, so then to file your returns after that, you have to have the PIN number to actually file that, so, you know, they've added another layer of authentication to get in there.

Steve Sanduski: Well, guys, I've saved the hardest thing to avoid getting attacked for last here.

Bill Keen: Okay. All right.

Steve Sanduski: Can you guess what it is?

Matt Wilson: Is it your cell phone?

Steve Sanduski: Sort of. I'll give you partial credit for that.

Matt Wilson: Okay.

Steve Sanduski: It's limit what you share online.

Matt Wilson: Yeah. Well, I think I do okay with that.

Bill Keen: Yeah.

Steve Sanduski: There's a lot of people out there who don't, who just love sharing stuff online. But it is important to just think about what you're sharing. You know, for example, if you're on a vacation and you're posting pictures on Instagram or Facebook about, you know, "We're in Paris right now." Well, if someone happens to be monitoring that, yeah, look, you know, the Smiths are in Paris right now. Maybe we ought to go break into their house. I mean, that's an extreme example, but, you know, it's an easy way for criminals to see where you're at.

And so it is important just to be very cautious about what personal information you're sharing, home addresses, phone numbers, birth dates, those types of things. And most of the services that people are using, whether it's Facebook or Instagram or Google, those types of things, they do have different settings in there where you can go into the settings and the privacy function and you do have control over how much you want to share and how much you're gonna let those companies track your every move on the Internet, so it does pay for you to take some time, get familiar with those privacy settings, and make a

conscious decision on how selective you want to be in terms of what information you're gonna let out there.

Bill Keen: What you're talking about Steve, a social media focus, too. Just what you're doing publicly versus, yes, if you go apply for a credit card, you're gonna have to put your personal information in that website to go do that and, you know, one of the tips that we have is always make sure, this is how you can confirm if you're using the right website is that if it's a secure website, is it's h-t-t-p-s at the beginning of the URL.

So if you're in Google and you're going to, you know, Schwab.com, you want to make sure it says https in front of that Schwab.com or any of those websites when you're putting in any personal information, birth dates, social security numbers, addresses, all of that, putting your credit card information in there. Always make sure it's a secure site.

Matt Wilson: I wanted to bring up one more because I mentioned mobile phones. I think I said cell phones. Does that date me as well? Are they called cell phones anymore, Steve, or is it just mobile phones? Is it proper terminology?

Steve Sanduski: I think they're called rotary dial phones.

Matt Wilson: Here's one that most people don't realize but it is starting to be reported. Cybercriminals actually have been able to take over some people's mobile phones, and impersonate them or actually reroute phone calls. Now that is scary but they say cybercriminals get the phone company to forward your cell number to their cell phone so they can impersonate you when your bank calls you back for verification.

Now how about that? I haven't heard anything personally, but we monitor these things in the reports that are coming in so the thing that we always recommend and, gosh, I know this sounds like you're going to have to hire a concierge full-time to just monitor all of your different touch points, but check your monthly phone bill for any suspicious activity.

And that includes phone numbers you don't recognize, calls placed at odd times, calls overseas or while you're on vacation.

Steve Sanduski: Well, let me just summarize a few things that we talked about here and then I'll turn it back to you two guys for some final thoughts in terms of what are we doing to do with this information? So, just some of the things we already touched on.

Take a look at your email systems that you're using, and implement that two-step verification process. Be very careful about clicking on hyperlinks in email so this is that whole phishing issue, so be very cautious about what you're clicking on.

Another one is to really think about the passwords that you're using and consider using one of these software password protectors that are digitally encrypted so that will help you to have more secure passwords and you won't have to remember all the different passwords that you use.

We also talked about looking at your bank statements, credit card statements, checking those right away, and making sure that you're with a good credit card company that has some automated systems to alert you if there's any type of suspicious activity in your account. So those are a few of the things we talked about, guys. Anything else that you want to mention there as we wrap up?

Matt Wilson: Yeah, another item is to always make sure that your operating system on your computer and your mobile devices are up to date because there will be software breaches, security breaches, that are identified from time to time and they will release fixes for those in that software update. So that is extremely important, especially on your mobile device, because those can get exploited and these hackers can get access to a lot of your personal information if they're able to get in there.

Bill Keen: I wanted to rapid fire a few at you. Wireless networks. Be sure to use wireless networks you trust and that you know are protected. Do you use the one at Starbucks when you're there that everybody else is on, or do you use your own? Do you bring your own hotspot from your own, let's call it mobile phone, that you hook to your computer? That's a question that I would ask.

Be cautious when using any public computers. There are times when you walk up to a computer and you log into your personal information at various places, temporarily. Make sure you log out when you are at those. Also make sure that you're not doing any banking transactions at any of those computers of any kind.

So, the last thing I wanted to mention is if you get rid of a phone or a computer, you've got to make sure that you permanently erase the information by removing and remove SIM cards and SD cards and those kind of things from your phone. So those things aren't floating around out there.

Steve Sanduski: All good stuff there, Bill and Matt. So thank you, guys, for sharing that. So final words?

Bill Keen: My final word is going to be a question to you today. It's going to be slightly different than how we close most of our episodes, we're going to end the episode with a question. And a quiz.

And that is going to be when were Social Security numbers first introduced?

Matt, you can join in because I know I'm catching you both off guard here. This is not scripted.

Steve Sanduski: Well, Matt, I see you looking it up on the Internet.

Matt Wilson: Well, you know, here's the funny thing. I was pulling up the website 'cause I had learned a little bit about the history of the social security number, yeah, the digits and the order, how they were assigned and so I actually had this pulled up so I kind of had the answer already, so I won't answer it.

Steve Sanduski: Okay. Well, I'm gonna guess 1937, because I think that is roughly the time that social security came into play.

Bill Keen: Alright. So if I had my sound equipment here, I would give you an applause. It is social security numbers were introduced in 1936 as a way to keep track- so you missed it by a year, but I'll give it to you-

Steve Sanduski: Okay.

Bill Keen: - of the earnings of U.S. workers for purposes of determining their entitlement to social security benefits. Now, I thought this would be an interesting way to close and it could have been an interesting way to open, but as quickly as 1938, so 2 short years later, the social security number as a unique identifier began to be a possible failure. And here's what happened.

A sample social security card included in wallets sold in Woolworths and other department stores back then ultimately resulted in as many as 40,000 people using the social security number of a secretary of a senior executive at the wallet's manufacturer. The secretary at issue was given a new number but for the estimated 60 to 80% of the Americans nowadays, even before this Equifax breach, whose social security numbers have been compromised, there can be years of anxiety and hassle, so I'll close today with the fact that, who knows, how much longer will we all have social security numbers to use, a unique number that, once compromised, creates a huge problem. We'll see. Only time will tell.

But in the meantime, folks, protect your data, protect yourselves, protect your family.

Thank you all, Matt, Steve, everybody, all our listeners for joining us today.