Cybersecurity Insights for the Sandwich Generation with Dan Krutoy

Introduction to the Sandwich Generation Survival Guide

Candace Dellacona: Welcome to the Sandwich Generation Survival Guide. I am your host, Candace Dellacona, and I am so glad to welcome fellow sandwich generation member Dan Krutoy, who is here to talk about all things security related to cyberspace. Welcome, Dan.

Daniel Krutoy: Thank you so much for having me, Candace. Real excited to be here.

Candace Dellacona: Yeah, I'm so excited too, so for our listeners, Dan and I work together with our clients and, we had a really interesting conversation that I thought would be useful to everyone out there as we navigate the world of cybersecurity and all of the things that we should and should not be doing for every level of our sandwich generation quagmire that we have. So Dan, you're the guy to talk to about that.

Meet Dan Krutoy: Cybersecurity Expert

Candace Dellacona: So maybe just fill us in a bit about who you are, who you work for and then we'll get into kind of the nuts and bolts of the topic today.

Daniel Krutoy: Awesome. Thank you again, Candace. As mentioned, Dan Krutoy. So my title is Principal for a technology firm called Pro4ia and I've been in every seat from a technology standpoint, from the support side, help desk, to more client facing, to strategic and whatnot. And as you can imagine, technology has evolved so much and changed. And that's what's exciting about being in this profession is it never gets stale. And that's what gets me excited in the morning, is talking about these different technologies.

Candace Dellacona: So having that bird's eye view I think it's really important for people to understand is that, you work with executives but you work with families as well. And the families that you work with are often concerned about privacy and security. And even though many people think that that issue only impacts a family of wealth, I think one of the things that we talked about as sandwich generation members is that it really impacts all of us.

Understanding Cyber Threats in the Modern World

Candace Dellacona: So what I would love to talk about today is because of the changing landscape and all of this incredibly rapid increase in technology and the scams that go along with it. What are the best words of advice and tips that you can provide to us to protect ourselves at every level? So can you talk a little bit about that in general?

Maybe let's talk about what the dangers are and then how we kind of prevent being a victim of those scams. So what are you seeing out there as kind of a trend?

Daniel Krutoy: Yeah. And it's a great point. And talking about families and talking about kind of personal outside of work technology it's so prevalent in, in every aspect of it. And there's so much overlap as well, right? You have your personal life that overlaps with your business.

But, going back to my earlier comment, how technology has evolved cyber threats used to really be focused on, the office space and, people would try to steal data there and you'd always have to lock your IT room or lock your computer or things like that. But now with everything being in the cloud now with everything being mobile and accessible. Your homes and your families and I'll use my mom as a perfect example, being that tech guy. I get a call, at least once a day or every couple days or a screenshot sent via text of, what is this? Or should I be clicking this? It's an update on my computer. Is this real or not?

And yeah, I think to answer your question is ask a question or ask questions. That's the number one thing is when we implement and ask clients or even, families to invest in cybersecurity, the number one thing outside of multifactor authentication, which obviously adds that human element, is awareness, training, and being aware of what you're clicking on, what you're doing who you're doing it with. That's the number one thing I would stress is making sure people are aware. Because you're so distracted by, your kids' homework and yelling at you while you're also working at the same time. That's the time that you click on something accidentally and now money's being transferred to another account, or now unauthorized access is happening to your computer.

Candace Dellacona: So let's talk about that and obviously those phishing expeditions that the scammers send to all of us. But I think you bring up a really important point that, there used to be a focus in the professional world and a concern about cybersecurity in the professional world, but it's really bled into everyone's personal life because we're all so technology minded.

We all are looking for ways to be more efficient and have all of our information in our phones and on our computers. And while it has made our lives I think better. And I don't think most people would argue with that. In terms of efficiency, it has opened ourselves up from a personal perspective of not having the tech guy, your mom is very lucky to have someone like you to be able to call at the drop of a hat and say, Dan, what do I do?

But are the scams that you're seeing?

Protecting Seniors from Cyber Scams

Candace Dellacona: And let's maybe start with the senior population. In terms of what people are dealing with, I'll just tell you quickly that I was a victim of a cybersecurity issue where someone somehow got a hold of my social security number and filed an unemployment claim, and I had packages apparently being delivered everywhere, and there were four credit cards open in my name. But are you seeing any particular trends that are being perpetrated against seniors?

Daniel Krutoy: Yeah, I'd say seniors specifically that you've probably heard in the news, there's scenarios where they get a phone call saying, one of your children is in jail and you need to wire this money to get them out or they get texts to their phone saying, here's a UPS delivery, you need to confirm your password so that it gets to your home. And things like that. Things that you know, look like day-to-day scenarios that they may not be educated on. And it happens in the moment and you don't really have time to think about it, is where they're targeting it.

And social engineering is like a buzz term in the industry because of technology. Information is available everywhere, right? So if I Google someone's first and last name, I can find their address, I can find their phone number, I can find so much information about them. And what they do is they use that as an opportunity to learn. What are their tendencies? What day of the week or what day of the month do they pay their bills? What once they get into their systems, it's not a matter of if it's when, right? So a lot of times we hear about attacks that have happened and it happened on, a certain day.

They've been in the system for like six months just watching what you're doing because they wanna understand the tendencies. That's what's happening. And also you've probably heard of solutions like software as a service or hardware as a service where you can pay, it's an operating expense where you could pay for solutions for a business.

There's now cyber security hacking as a service, so a bad actor can go online and for minimal amount of money they can buy a piece of software or a package or a tool that empowers them to go out and, go after people, right? It's a numbers game. If they send out this campaign or whatnot to thousands of people, all it takes is one to click on it and now you're in trouble.

Candace Dellacona: Yeah. So when you talk about social engineering you're essentially saying these bad actors are mining our social media profiles to get information on us. Is that it?

Daniel Krutoy: That's exactly it. You've also heard in the news, right? Facebook was selling people's information and all of these other websites. Now, when you go on any website, they ask you about cookies and do you have to accept or you can't move forward until you accept a certain amount of data to be allowed.

That's how these websites make money. They sell your data to all these third party, broker sites or whatnot, that now, it's used for marketing tools, but it's also used for, bad activities, so to speak. Yeah, that's exactly it. When you're on Facebook, when you're on Instagram, when you're on social media, when you're shopping online, all your information is now out there. And at some point it's gonna eventually be available to somebody that wants to do something.

Candace Dellacona: And look, we all like to be connected through social media, whether it's, Facebook or Instagram or what have you. But let's talk specifically about the social media profiles and I think most of the listeners would agree that most people feel that they enjoy that part of connectivity with their loved ones or their friends that perhaps don't live close by.

And, maybe for this, the home bound seniors, that's a way that they can keep up with their grandkids or keep up with family members who live across the country or out of the country.

Social Media Safety Tips

Candace Dellacona: So how would you suggest just taking it from a social media perspective? That you would come in and help a client, quote unquote clean up what's in their social media profile to give less opportunity to those bad actors. What are the tips for us?

Daniel Krutoy: Sure. It's hard to say. But I think the common knowledge around it is, the less information, the better, right? If you wanna post a picture of something, that's great, but when you post a picture of something and where you are and what you're doing right, that gives people kind of an idea of, oh, they're in Cancun this week. That means they're not home. And I can Google this person's address and next thing you know, there's theft at they're home. It's a double-edged sword, right? You use social media because you wanna socialize and you wanna share what's happening in your world. But people also use that against you because now you're sharing a little bit too much information that they otherwise would've not known is happening. There's two aspects of it, right? You can secure your data and your information, right? You don't want somebody going into your Instagram account and hacking it and then sending things there so that you can do that's, put multifactor authentication on it. Make a complex password, change your password every six months, because a lot of people use the same passwords for multiple platforms. So if they get into one system, they're most likely gonna try all the other systems. So while that's a bit of a nuisance but it takes 10 seconds versus if someone hacked into your account, now you're spending countless hours trying to get back into it or things like that.

So that's the data aspect of it. But now the social kind of engineering that we talked about it is, that's really a conscious decision on the individual. How much information do you really wanna give that you're, traveling somewhere or that you're doing something or that you bought a new piece of jewelry and you'll see random things of people sharing things that they're doing. And that's really that's up to that, the individual.

Candace Dellacona: Yeah, I think that a lot of people struggle with that in general. And I think that, oftentimes we think of the outside world in ways that why would anybody care what I'm doing? I couldn't possibly be the one to be hacked. And having gone through it it definitely was a wake up call for me.

And I will also add, that the tagging of other people, I think should be thought about with some care. A because other people might not want to be tagged in a particular location or at a particular event. But I think, based on the situation that you bring up where the phone call comes in for the senior and it's, the caller on the other end is saying, your grandchild is in jail and they know your grandchild's name because you've mentioned them and the social media post.

It is a hard lesson to, to learn. And there is a tension there between the connectivity and, feeling like you're up on the events of your loved ones and your friends. And also being mindful that unfortunately there could be people lurking in the background that perhaps don't have your best intentions at heart.

When you think about cybersecurity for those who are in that older generation, and you talked about your mom, so not clicking on things is one of your words of wisdom. And I think that's a good one. I've also been guilty of doing that once in a while, being distracted and just trying to multitask what are the other things that as children of the older generation or the nieces, nephews, the quote younger for those of us in the middle, how can we set our parents up in such a way to protect them even if they're out on, social media and they're posting things. What are the things that you share with your older clients as it relates to their own cybersecurity?

Daniel Krutoy: Yeah. Great question, and I'd go back to the core function of it is education. You gotta educate them on what they're exposing themselves to by doing all these things. So I'll give a perfect example. I'm sure everyone you speak to in the older generations like, AI this thing is coming and I'm definitely not touching, I'm not getting involved, yada, yada, yada.

But next thing you know, they're using Waze, right? Waze is their GPS and that's AI. They're using AI and then they say, alright, fine. That's not a big deal. And then they log into their bank account and they're doing facial recognition. That's part of AI and that's part of biometrics and technology and all these different things. So whether you like it or not, or whether you wanna accept it or not, all these different technologies that are available to you and that you're playing with are have some form of all these new things that are involved. So you have to educate them on it. The other thing I would say is, sit down with them and every single app that you use or your iPhone or things like that, you have to really drill into the settings and the cyber and security aspects of it, right? Because it's not just one button on or off, like, Hey, I want cookies, or, Hey, I don't wanna share my information. There's so many different settings, like location like tracking your information, all that other stuff. So sitting down with them and, if they're using Facebook, go through all the Facebook settings and one by one, go through all these.

Do you wanna turn this on? Turn this off. That helps from that standpoint. Someone shared with me Gmail recently was exposed or information was shared that you have to go into Gmail and turn off a bunch of settings. Otherwise they're gonna share all of your, personal information as well.

So, educating them staying up to date on the new threats that are out there. I think that's the number one thing. And then I'd say on a bare minimum, I mentioned this a little bit earlier, so multifactor authentication,

Candace Dellacona: Yeah. Can you go into that a little bit about what multifactor authentication is for, a lot of people I think don't know that.

Daniel Krutoy: Sure. So multifactor authentication's kind of the full terminology a lot. It also goes as 2FA or MFA. So two-factor authentication or multifactor authentication. So when you type in your password, if you don't have MFA turned on, then if somebody gets your password, they type it in from anywhere and then they can log in. What multifactor adds is that second element, that human element of, okay, I got your password, but now I need to authenticate a second way that requires human intervention. So let's say that bad actor stole your password. You're located in New York and they're logging in from, Russia. They need your phone or they need that code to be able to go into it to get there. Or there's other methods to just have that second factor.

So turning that on and you'll see majority of the websites, like banks and whatnot, they required at this point, you can't even turn that feature off because, over 90% of breaches are because of password compromise and someone let somebody in through the back door. So, I'd say make sure that that's turned on for everything, and that helps a lot of the ways. And then the awareness that I mentioned, just making sure they're educated on, if something doesn't look right just call, call your grandson or your daughter or whoever and ask them did you send me this? Or should I click on this? Should I open this? And it's links. Don't click on links that you're not familiar with. Even attachments can have, some kind of thread in it. Even if it's from somebody that you know, that person could have been compromised. And what they do is a trickle down effect is they try to compromise everyone within that person's contact list. So then they send a link.

So you have to be careful no matter what. And then as part of phishing campaigns it's very simple to, change one letter or one digit in someone's email address, right? So, if you have Candace in your email instead of an E, sometimes they put a three at the end of your name.

Or let's say you own a .com, they can change the Gmail. Obviously that's a bigger one, but they could change an I to a one or things like that. So they try to manipulate you in different ways. So it's really just trying to be aware as much as possible.

Candace Dellacona: As with any sandwich generation issue, I think, communication is really key. And as we embark on this holiday season, you bring up a really good bit of advice, Dan, which is to sit down with your aging loved one and go through their phone with them and really take a look at the settings on every app that they have.

And it sounds like there is a way to go through and make sure that the app isn't tracking and that there is only necessary cookies and things like that. I think as a novice myself, I didn't actually realize that the cookies request was not only for marketing, but also to sell your information.

I really did think it was just for marketing purposes. I'm proud to say that I always say no, but you're right. Like even these little sort of subtle click and dialogue boxes that come up, we all have a tendency to just kind of rush through them. So slowing down, taking a look at the phone, looking at the settings with your loved one, and having the conversation about not clicking.

And I think that leads us to the next generation, which is okay now our kids, where in many cases, maybe not yours, but our kids are more technologically savvy than a lot of the parents.

Cybersecurity for Children and Teens

Candace Dellacona: So can you talk about what you've seen in terms of, influences and things that we should be looking out for or tips that you can provide for parents looking to secure their children in the world of technology?

Daniel Krutoy: That opens up a whole other can of worms, right? It, once again, it becomes a choice. And the challenge is, I'm a parent of a 9-year-old and a 7-year-old, and the conversations are already starting of, when can I get a phone or can I have a phone? And you have the holiday season coming up and birthdays and it's tough, right?

Because it's not just the individual conversation between you and your child, it's also, the peer pressure of, I'm in school and some parents allow kids to have phones at a certain age and some parents don't. And now you're fighting two different battles of that. So I don't want to go down the road of, what's right or wrong. 'Cause there is no right or wrong answer. But what I would say is back to a similar answer for the elderly is if you do get a phone for your child, Apple and iPhone, I could speak to that specifically. I'm not a big Samsung or Android phone user. I'm sure they have similar settings. You have sort of that parent child mode. And we actually did use that when we did send my kids away to camp and they were gone for the entire day. We did want to track them, we did want to be able to communicate with them. We were able to lock the phone down completely so that they could only send and received phone calls and texts from people in the contact list.

So myself, my wife, grandparents and whatnot. So if anyone tried to contact them from the outside, it wouldn't go through. And then also if they were communicating, with a grandparent, I could also see that text as well. So let's say, God forbid a grandparent's phone was stolen and now you're communicating with a child, you're at least seeing everything that's coming through. And it allows you to, authorize any apps that they download, right? If they want to play a game, you have to approve it. If they want to go to a website it's locked down by default. You may wanna open up a certain link that they can go to. So Apple definitely has all of those features that you can employ.

Candace Dellacona: And that's amazing because as a parent of older kids to my knowledge that was not available all the years ago when my kids got a phone. I mean, certainly the rule in our house and as you point out, there is no right way. So, I don't wanna get any emails about, my way is definitely not the right way.

It was just worked for my family is we would take the phones often at night. And plug them in and certain things were not private in our house. And so that was sort of the way, it was like maybe the old fashioned way of going through things, but I didn't realize that there was an actual setting with certain providers that would allow that kind of ability to put a protection around your kids. So the phone is one thing. What about being on the computer? Are there similar settings, Dan, that you recommend in your house where you say, okay, the kids can do X, Y, and Z, and how do you go about doing that?

Daniel Krutoy: So whole other challenge and something that comes up all the time. My kids personally get Chromebooks through their school that allows them to, they use it in the classrooms for, various activities and learning and whatnot. And for the most part it's locked down, so they can't really do too much outside of what that platform is allowed. But without speaking with too much knowledge, I hear my son and some of his friends talking about, there's. VPNs and special ways that they try to work around and try to get to certain websites outside of just the ecosystem that the Chromebook has allowed. So I think once again, awareness and watching what they do it, it's tough, right?

You can't sit there and watch every single moment that while you are working and maybe they're on their Chromebook and have a certain amount of screen time. Making sure that it's locked down and making sure that you're observing. So when they're done for the day, like you mentioned, you would take your kid's phone and charge them. You have the ability to go in and look at the history if they went to certain websites or getting redirected to certain websites. But that's the school version of it. If you have personal devices, the one thing I would definitely say is, work computers should be completely separate from, personal computers because there's a line of delineation there. You don't want to mix and match, but it's hard. I know it happens and a lot of companies actually employ, bring your own device, so you can't really stop that from happening. But if I could give you a best practice or recommendation, I would say your work computers, your work computer, your personal computers, your personal computer.

And I'm not saying you can't shop on Amazon. I'm not saying you can't go on websites, but if your kids are gonna be using it and they're gonna be going to certain games and gaming sites and things like that, you just don't want to take that risk. So if you do have that device where they're using it just for personal use, there are settings in there for sure that you can lock it down and windows or Apple allows you to say, all right, this is a child of this age and there's a bunch of options you can toggle to say, certain category websites they definitely can't go to. Or they predefine them for you. If they're within a certain age range, they can go to certain websites. And then it's up to you as a parent if you want to granularly say, all right, this site's okay, but that site is not okay.

Candace Dellacona: No, I love that there is the infrastructure already that sort of set forth within the technology, whether it's, Apple or Android, that you do have the ability to reign it in. I think you probably have seen the news that Australia, I think is the first country that has now locked down social media sites for kids under 16, which, I think is pretty bold.

And I really admire the intention behind it. It'll be interesting to see if it is able to be enforced and if something like that is possible in our country. But until then, having the mechanism in the device to try to control those outside features, so that you can protect your kids or your elderly loved ones as much as possible.

What to Do If You've Been Hacked

Candace Dellacona: I guess my final question for you is, let's say, the horse is out of the barn, as they say, and you have been hacked. What are the measures that you recommend as an IT professional to try to repair and set yourself up for success so that it doesn't happen again?

Daniel Krutoy: Sure. I guess there's a couple parts to this question. From a business perspective, if we're looking at it, if something, a compromise has happened, let's say to a computer, first thing you do, unplug it from the internet, right? Get it offline so it doesn't spread any further. If it's an account, like a user account email account or something that you log in with. Immediately try to secure that account. And when you say secure is change the password, make sure if you don't have multifactor put it on there or reset it so that it's just, locked in. From a personal standpoint same thing. If it's a computer, I would unplug it from the internet and isolate it from that standpoint. If it's your email accounts or some kind of login. First thing you need to do is change your password immediately. Even if it's like a randomly generated password of like 16 characters with symbols and whatnot. Make it as complex as possible. A lot of these tools and systems when you go in, they have some kind of logging feature. So you want to see who's logged in or kick them out if you can or things like that. And then I would obviously call a professional. And when I say professional, it could be, a child, it could, or your son or daughter, I don't mean a little child, but someone that, has some tech background or ability and work with them.

And then, yeah you basically have to find the root cause. Is it just isolated to my Facebook account? Is it my bank account? Once you figure that out, then you gotta make the phone calls to those places to make sure that it hasn't spread any further. Run scans on those machines with antivirus and whatnot. But if it's something bigger where it's financial impact or others, I would probably get a professional involved.

Candace Dellacona: Yeah, I think that that's great advice. Look, as we said at the top of the episode, technology is pretty amazing because it can offer us efficiency, it can allow us to connect with people who aren't around the corner or in the same house. But there are also pitfalls that we have to be aware of.

And as with most issues that we deal with, the sandwich generation, communication I think is key. So I'm really grateful for you sharing the inside scoop today. I know that you deal with many more complex things, so I appreciate you breaking down the simple things for our audience today.

Daniel Krutoy: Yeah.

Final Thoughts and Future Concerns

Daniel Krutoy: And can I give one more piece with AI and someone actually mentioned this in one of the business groups, actually a similar group that you and I are in. That with AI, your voice recording within three seconds would be able to use that as a voice recognition for a multifactor authentication that allows you to unlock an account.

And I think three minutes is what they said. If they record you for three minutes, they can basically replicate your voice to do a full conversation and whatnot. And that's just today. So imagine a year from now and further on.

So not only to break into accounts, but those phone calls to the elderly, they can be using the voice of their child or grandchild saying, Hey, send me this money. And that's a really scary thing and I don't know what the right answer is today, but I'll leave you at that.

Candace Dellacona: Yeah, So thanks for leaving us with the most frightening thing I've heard in a really long time, and particularly because, as a podcaster, I think my voice is out there, i'm gonna end up having to hire your company when something like this happens again. But, I'm really grateful for all of your advice and even if it's troubling to know what's out there, I think half the battle is knowing what's out there so that we can protect ourselves.

So thank you so much, Dan, for joining us today. And all of your contact information will be in our show notes for all of our listeners. Thanks everyone.

Daniel Krutoy: It was great to be here. Thanks so much.