[Transcript] Shared Security / Special Guest Jayson E. Street, Phantom Hacker Scams, 23andMe User Data For Sale

You're listening to Shared Security, a podcast that explores the bonds shared between people and technology, hosted by Tom Eston, Scott Wright, and Kevin Johnson.
Welcome to Milestone, episode 300 of the Shared Security podcast.
Joining me this week are my co-host, Scott Wright and Kevin Johnson, as always, but we are also joined by very special guest, the one and only Jason Street.
Yeah.
Welcome, Mason.
Thank you for having me.
I greatly appreciate it.
You know how to know he's the one and only, right?
The Y in his name.
Exactly.
That's how you know.
That's right.
If it doesn't have a Y, if it doesn't have a Y, it's a Timu knockoff.
And quite a few, and I always leave people wondering why it's like, it was perfect.
That is perfect, actually.
That is awesome.
So if you don't know Jason, so Jason has actually been one of our frequent guests, actually, going way back to episode 63, which was back in 2017, was the first time that Jason was on the show, but he was also on the show for our 10-year anniversary episode, which was back in 2019.
So basically, every couple of years, we invite Jason back for one of our milestone episodes.
So welcome back, Jason.
Really glad you're on.
Well, I'm glad.
Yeah, it is true.
I'm only good in small doses, so you've got to spread it out.
It's like, I understand.
Yes, yes, yes.
Well, we're doing that for so expensive, we can't really afford to have them very often.
There you go.
That's right.
So speaking of Jason, Jason, there are a lot of stuff going on, right, since DEFCON and all of that.
Yeah, it's been crazy.
The training I did at DEFCON was like amazing.
I was very happy about that.
Then I was laid off as soon as I left DEFCON, which was not the greatest in time and everything.
And then I flew to New York to do a Wired episode, which was hilarious.
I wish it would have released it a week before because a week after they released it, the MGM thing came out.
And you can see in the video me talking about what I do with LinkedIn and how I use it and

stuff.
So I was like, ah, so close.
And then I was literally blessed and just so, so happy to get a landed job with Security as a Chief Adversarial Officer for them with Casey and the whole team there, Brett and everybody.
It's like they have got some heavy hitters, Steve Fink, Craig Miles, Dark Matter.
It's like, you know, Wi-Fi Cactus is good, it's there.
They've got some really good heavy hitters.
They're a really good team.
It's like we did a lot of like negotiation at the very beginning because I told them, it's like, look, it's like, don't hire me just for a name and then not know what to do with me.
You understand?
It's like, this is the things that I do, this is what I'm good at.
And luckily Casey knows I was a horrible employee to begin with.
So there was no, no expectations, exactly.
So it worked out.
So and I'm enjoying it.
I'm like having so much work doing.
It's like I'm doing a talk in a couple of weeks.
I've already done a couple of other projects.
It's like, I've got to rob some.
I haven't robbed anybody in so long.
So disappointing.
So I finally got, and I've got the, oh my gosh, I can't say it publicly, but I've, I registered two websites, a dot MOV and the dot zip, and they are as horrible and as malicious as you're thinking.
Oh no.
And I finally get to use them when I'm robbing someone.
It's like an efficient attack.
And it's like, I get to do a vision attack coming up.
And it's, and it's so like chef's kiss because it's, it's deemed over security like so telling people like, you know, you need to be aware of these kinds of things.
Go check out this site for more.
And that's the malicious link.
It's horrible.
It's horrible.
It's horrible.
Nasty.
Yes.
That's good.
Well, hopefully you'll be able to tell that story, you know, after, you know, you can disclose more info about it, but I would love to bring you on.

Next time.
Yeah.
Yeah.
Exactly.
And maybe it won't be five years.
Yeah.
Who knows?
We'll see.
So do you have anything else coming up that maybe you want to talk about besides your super secret linky thing?
Yeah, I'm just doing a, I'm going to be in Boston in a couple of weeks, speaking at the Tyler Tech conference, I believe.
And then I should be, it's still up in the air because I haven't heard back from them in a while, but I'm still on their website, even though my name's misspelled because why?
Yeah.
In Sydney, Australia in November, so to the CSI awards.
So really happy for that one.
I've never been to Australia before, so that's going to be fun.
But this year, I'd really just, I got so burned out from last year is like that I was traveling like out of the country at least twice a month, almost the whole entire year.
And after December, where I was in summer in South Africa and Cape Town.
For a week and then flew directly to the Netherlands to deal with the winner for a week.
I was just like, I'm taking all the January off and it's like, and then I'm going to only do one country a month for the rest of the year, if at all.
And so I've kept it really slow this year.
Next year, I'm pretty sure it's going to speed up because I got some new research stuff that I was going to do.
I've got this new, I can talk about this attack, it's a really cool attack where I want, I'm talking about common attack tools, not a sophistication and human intelligence, not artificial intelligence.
It's like, my talk of my title is something like, you know, the new move over AI, the new hotness is H I, it's like, which is human intelligence, like, let's, let's, you know, cultivating and developing that instead of trying to develop AI.
And so it's this attack is you get a drone.
It's like $100, maybe $200, right?
It's like a small investment to pay to get a micro that has a micro SD card in it.
And what I do is around 930 to 10 o'clock at night, I fly it into the building.
So it crashes.
It's like by the front door or by the security gate, if possible, and what is going to occur?
Finding a USB drive, they're going to investigate it.
They're going to go, Oh, there's a drone.
Someone was doing SP not someone was doing something.
They're going to take it in.

They're going to open up the micro SD card.
There are two files.
One is a Word document that states it's like pilot and FAA registration number.
It's like document.
And we know what happens when they click on that.
And then there's a like a DJI dot zero does that, you know, EXE dot MOV.
It's like, and if you click on that, it opens up to Rick rolling you.
And then you close that window and it says you've been pwned as a pop up.
And it's like, because it's like either file will.
So you make your employees, you weaponize their curiosity and just they're thinking like, well, it's a drone.
Why would it be something like an attack tool?
Why would it be a threat?
It's just a drone.
That's brilliant.
Drone.
Yeah.
Yeah, sure.
It's a honey drone.
Yeah, exactly.
I'm not.
I'm not.
I'm not technical.
It's like, I'm very, I'm very good at indivious when it comes to like circumventing humans and compromising them.
Yeah.
I think that's a great way to break into Waffle House, Kevin.
There you go.
Because they'll shoot the drone out of the air before it gets to the drone.
Two things.
One, they won't shoot the drone.
They'll throw a chair at it.
And two, there's no reason to break into Waffle House.
They don't lock the doors.
That's true.
That's true.
That's true.
Good point.
Well, that's awesome.
So Jason's here to kind of be our guest host and he'll be commenting on the two stories that we're going to talk about.
So I am, I'm looking forward to this.
So Scott, why don't we jump right into our favorite segment, which is aware much.

Okay, I just, I have to share, sorry.
One of my staff is a loyal listener and he listens all the time and he did comment after last week's episode where I guess you said that it was so quiet when you did the aware much.
I wasn't there to laugh.
Yeah, you weren't.
And he said, they're right it was.
So, so Josh, I listened.
Well done.
Yes.
Thanks, Tom.
And yeah, it'll be interesting to hear Jason's comments on this section because this is about a scam.
It's a social engineering scam, mostly done by telephone.
But it targets seniors typically.
And so I don't know how often Jason targets seniors or is hired to target seniors.
But that'll be interesting to hear.
But this is a really kind of more sophisticated version of scams we've heard before starts with a tech support scam gets the victim to install malware on their computer remote remote access malware.
And then they sort of scout around to see if the person's worth attacking further.
And then they phone them as a representative from a bank or financial institution saying there's been a hacking attempt on your account, please move your money to a secure account.
And if they don't go for that, then they get another call later from the government saying, we really encourage you to move your money into that safe account.
And this apparently has resulted in about $50 million worth of complaints to the FBI.
So really a very insidious kind of attack and I'd love to hear what you guys have to say about that.
Well, right off the bat, if I may, if they've got $50 million worth of complaints to the FBI, that's the start of the number that it is, right?
Yeah.
Because that most people reported.
Yeah.
Exactly.
From my experience doing expert witness work for the Florida Attorney General's Office on cases like this.
The majority of people don't complain.
Many people don't know that they got hit.
And if they do figure out they got hit, they don't think there's anything they can do.
And so they, or they're embarrassed or whatever, and so they don't complain.
Actually I was wrong.
10 times that, $540 million.
That's worse.

That's worse.
Yeah.
Yeah.
That's worse.
It is worse.
I would say I always tell people there are, one of the key things I tell people, especially when they're talking about like doing things on their machine.
It's like, I've always recommended, spend $100.
It's like, and buy a net book.
A literally cheap, bare bones Chromebook that gets the internet.
And I tell people, and I tell this to executives, to school, I tell it to anyone.
It's like something I do.
It's like, and you put just, you don't put any games, you don't install anything on it.
Default web browser, you type in the names to your bank, your bill pay, all those different services that you involve with money.
And you put that on that machine.
And you only use that machine.
You don't install email on it.
And if you've got a, if you like mobile payments, because you know, a lot of stuff is just, I don't, sort of the mobiles, carry it.
I carry a second phone.
It's like all my apps and stuff that are banking or like you're on that.
I don't have text messages.
I don't have all these other things on it, but I can do, you know, the pay, the electronic pay with it.
The tap to pay.
It's like, and you segment that.
So that way, even if they get your email or they get your social or they get your other things, they cannot connect to know what your bank is.
They can't connect to actually see that you have anything there.
And then you just, every month when you need to do bill pays, you open up the machine, you use it, you close it, and you put it back in the drawer unless you need it again.
As long as you remember never to do your banking on your regular internet surfing machine.
And that's, and that's the issue I see with this is, I think that's a great idea.
If it's possible, not if it's possible.
It's always possible.
But the bigger issue I think is actually in this story, no, not even with convenience.
The issue here is with this story, they're calling the person on their phone.
They got the access first.
No, no, no.
They researched the person.
Well, there was a call initially like a tech support.

Oh, okay.
To get the remote access.
Okay.
There you go.
Yeah.
Oh, on that, I would, yeah, that is hard to do because it's targeting seniors.
Yeah.
It's like, that takes people that are like, if they have someone in their life, it's like, they take someone to tell them, it's like, say, Hey, if you get any kind of call that is asking for anything to do with computers like that, you tell them they have to go through this person.
You give them another out because the problem with most seniors is they don't have permission to be rude.
Yeah.
It's like, they don't have permission to be not helpful or polite or kind when someone is calling them.
So you need to give them that permission saying, Hey, you tell them that you don't have any authorization to do any of that and that they have to, that you, and you don't give them my number.
You tell them that you need to record their information down and they will have someone get in touch with them.
So you're still helping them.
You're still wanting to work with them.
I like that idea.
It gives them a, it gives them that break and that breather to do that kind of thing.
So it's not a technical fix.
It is a human fix where it's like, you give them permission and I talk about that a lot when I, when I'm talking about how to empower our employees is that we don't empower our employees to let the management be the bad guys because employees, malicious insiders are not your threat.
Helpful employees are your malicious or your insider threat and it's like, and so you got to give them that permission to be impolite and say, no, I would love to let you in the door or I would love to answer these calls or help you out, but my manager or my children or my caregiver, they're horrible people.
They never let me do anything.
They don't give me access to any of this.
They're real jerks.
I love that.
I would love to help you, but I can't do it.
And let me tell you about, cause one time I had, and then just go off on tangents on them and it's like, it's like, just like Kit Boga.
Have you ever watched Kit Boga do his scambaiting?
Oh man, scambaiting and John Hammond does that.

But that's what I would do.
It's like, I think that would be the best way of like, it's just, and it's not technical.
It just sounds like, look, just tell them that you have to refer to somebody and just give them, it gives you a breather.
The simplest explanations or instructions are the best, right?
Yeah.
Yeah. Excellent.
Yeah.
So a great story.
We'll have a link to that in the show notes and there's some good tips there, which are more technical than what we were just talking about.
And it's, you know, they're all good tips, but can you get seniors to remember them?
Probably not.
So keep it simple.
So this episode of the security, sorry, the Aware Much segment was brought to you by Click Armor, which is really the most effective way to do remediation for security awareness programs.
Our fakes and frauds module will actually teach employees through interactive, choose your own adventure scenarios, which are gamified.
So if you have employees who have been identified as being vulnerable to fishing, social edging, or engineering, or other threats, then visit ClickArmor.ca and start a live chat to find out the right solution for your organization.
That's it for this installment of Aware Much.
All right.
Last story of the week, and it's about 23 and me.
Their data is up for sale after it was scraped through a credential stuffing attack.
We talked about credential stuffing before, but this is a big one.
This is actually millions of people have had their data exposed.
And to make things even worse, there were certain groups of people that looked to be targeted as well out of this attack.
So it brings up the question again of credential stuffing.
And of course, the response from 23 and me is like, hey, it's really not our fault.
People should choose better passwords.
And I personally think that is a poor response for a company that, you know.
Here's my issue with that.
I agree with you, it can be a poor response.
But the question becomes, how much could they have detected?
And what I mean by that is, if the attack are logged into millions of accounts from one IP address or 10 IP addresses, that is 100 percent something 23 and me should have detected 100 percent, 100 percent.
But you and I all know how easy it is to spin up a source to hit one account, right?
And log in and then spin up another IP and log in, spin up another IP.
That costs almost nothing.

So if, and I don't know, but if that is what happened, right?
The all of these logins happened from multiple IP addresses.
How much should 23 and me have been able to detect?
I will say they should have still detected it quite a bit.
And also you can't complain about the user's passwords when you're not creating a standard that would be more secure.
I disagree with that.
You can tell them that the, the length of the password has to be this long and there has to be a special character and that there has to be a number and you can allow spaces.
How many frigging websites still don't allow spaces?
But wait a minute, Jason, the issue here isn't that they had weak passwords.
Well, I thought that was how I just said it.
Am I not?
What they said was credential stuffing.
Yeah.
They used the password somewhere else, right?
Oh, okay.
Reach passwords.
And 23 and me, I'm a user of 23 and me, I have an account.
My wife has an account.
That's actually relevant to this because my wife is a, I should cause, I can't say it.
Ashkazi.
Right.
And her account was not compromised.
All right.
Or at least is not in the records we've seen.
Well, hopefully she got duplicated.
Yeah.
She's probably one of the people that are not doing password reuse.
She's not.
But here's the thing.
Again, I don't know that this is what happened, but if the attacker used multiple IP addresses, and I'm talking like one IP per account, I disagree that 23 and me shouldn't see that.
Why is that any different than me logging in from a different IP?
Quick question for you then, Kevin.
Would it not have been at least some detectable increase in the number of failed logins during a period of time?
If this statement is the person reused their password, there wouldn't have been a failed account.
Well, not every password reuse is successful, right?
I agree with that.
But every time I go to log into my account, I type out my password until I had a password manager, like a failed log.

Yes, there could have been an increase, but if you, as somebody who has been analyzing logs and dealing with this, if what we saw, and I'm not saying this would have happened,
but if what we saw was, all of a sudden, we had a 100% increase in failed login attempts.
But every one of those failed login attempts came from a different IP address.
Why should we have seen that as an attack?
Maybe we should.
An anomaly if not an attack, yes.
An anomaly absolutely, right?
Just like if all of a sudden we saw a million people log in when we tend to see 100,000 people log in.
Yeah, maybe it was a big commercial for 23 and a half.
It's an anomaly, but it doesn't mean it's an attack.
And my question is bluntly, if I was 23 and me, I would force every one of my accounts to have two factor.
I would have forced every one of my, right?
That's where they should have done that, but that's a proactive thing that has nothing to do with whether the breach is a factor.
Detection, yeah, yeah.
This is what happened to Ring, if you remember.
Exactly.
All those Ring cameras got hacked.
It was the same thing, was they didn't force people to use two factor authentication that kept it as an option, but no one's going to choose that option.
And as a Ring user, God, I'm just announcing everything.
Yeah, you are.
Wow.
Not only did they not force you to use two factor, it was difficult for me to figure out how to turn on two factor when I created the account, right?
Nowadays, it's an immediate, like it's easier, but when I first started it, it was awful trying to set that up.
And that absolutely is the company's fault.
That is absolutely the problem.
I don't like to second, you know, second, yes, armchair quarterback.
It's like without a lot more information.
I mean, like, I don't know exactly what's going on with 23 and me, but I will tell you, it sounds, I find it very hard to believe that it was, that they were being that sophisticated and using multiple IP addresses and doing these things.
I find that hard to believe as well.
And so, and so I get back to the point that you have to do exfiltration monitoring.
It's like Sony lost 1.8 terabytes and didn't notice it leaving their network.
That's an issue.
It's like, and so I think, I think 23 and me should have noticed that kind of exfiltration going on because the attack, I don't know that many criminals that are all about

patience and being subtle and like going, oh, let's just do it very slow.
We don't want them to know that we're getting against it.
No, they were going, they probably got it as fast as possible before they could get detected.
And why that is one of the problems that I see in a lot of the organizations is that they've got so many different rules letting you before you can get into their network.
But if you want out, mother, just go.
It's like, it's out.
It's like, we don't care.
We ain't looking.
It's like, and that's a problem.
Absolutely.
I apologize.
I need to drop.
Yeah, you can drop.
No worries.
I want to say, Jason, it's great seeing you again.
Great thing to do.
Thomas Scott, it's always good to see you guys.
I hope to see people in a IC squared security congress or a Wasp app sec.
Enjoy the Waffles.
Oh, I'll enjoy the Waffles again.
So yeah, Tom and I are doing a Waffle House Wednesday at IC squared.
Bye, everybody.
All right.
And I think that's a good, good place to end the podcast since Kevin's got to drop.
Kevin's got to go.
Yeah.
Thank you, Jason.
Thank you, Scott.
Thank you, Kevin.
Great to talk with you again, Jason.
And we'll talk to everyone else again next week.
Episode 301.
Thanks, everyone.
Y'all take care.
Thanks for watching or listening to this episode.
Please subscribe wherever you like to listen to podcasts and visit us at sharedsecurity.net or on X at shared sec.
If you'd like to help support the podcast and get early access to new episodes with no ads, plus many more exclusive benefits, become an official supporter of the podcast for only $5 a month.
Visit sharedsecurity.net slash supporter for more details.