

**Kerrin Mitchell**

Hey, what's up, Untappd philanthropy friends? We are talking about cybersecurity this month. We are so excited to have one of our dear friends and a colleague of mine here at Fluxx, Chris Aurelio, on the call. He is going to chat with us today about all things cybersecurity, lot of privacy, the things that you all hear about that obviously you know sometimes takes a level of translation to be able to understand what it means to you and how to apply it to your day-to-day work.

It was cybersecurity month in October. This feels like a ripe conversation, Tim, that we should be having, not just now, but often. So maybe, Chris, like, we're just going like, make you come back all the time because this is becoming something that is so, so important for our folks.

**Tim Sarrantonio**

Yeah, unfortunately, I think we need to continue to hear about this, so...

**Kerrin Mitchell**

I know, right? We're like, every quarter is cybersecurity quarter.

**Tim Sarrantonio**

Mm-hmm.

**Kerrin Mitchell**

Every month is cybersecurity month. But Chris, thank you so much for joining us. Welcome. You and I work together at Fluxx, but I'd love for you guys to give, ah for you rather, to give a big um kind of summary of who you are, your background. And we definitely have about a zillion questions for you that we'd love to explore today. But first, maybe some context for the listeners.

**Chris Aurelio**

Yeah, absolutely. I'm happy to be here. I have been working in information security for over 15 years across a range of industries and companies of all sizes.

For about 12 and a half years or so, I was focusing on leading security and in some Fortune environments and overseeing a global portfolio and just ensuring robust protections and compliance.

And now I am bringing my deep expertise to Fluxx to to help with all things

**Kerrin Mitchell**

Amen, brother.

**Chris Aurelio**

Security, privacy, and compliance related. so yeah

**Tim Sarrantonio**

Thank goodness.

**Kerrin Mitchell**

Awesome. Yeah. And I mean, I think in general, one of those things that cybersecurity can feel very intimidating to most people, and especially right now where it's coming at them from all angles. They can see it in even their consumer day-to-day life, the text, the spam, the million things, and it's only getting more complicated. So it's very abstract to many of us, but something you sort of clicked into very early in life and something that you actually built a path around ah How did you even get to the place where you were like, wait, this is not just something that is important for me and I find it exciting. But what sort of compelled you to say, I'm going to take this on? Like, this is my, this is my calling.

**Chris Aurelio**

Well, it's funny, it actually started with art when I was a kid.

**Kerrin Mitchell**

Oh, cool.

**Chris Aurelio**

So art has always been really a big part of of who I am

**Kerrin Mitchell**

Cool.

**Chris Aurelio**

You know how I've explored the world growing up. And I was always drawn into that creative process, you know seeing different patterns and solving problems and just kind of creating something from nothing.

So when I first discovered hacking, it felt like this extension of that same creative instinct. It was... you know, a different medium, but that same artistry.

And eventually I came to realize it is, yeah, absolutely.

**Kerrin Mitchell**

And complexity in that sense too. Yeah. Interesting. Yeah.

**Chris Aurelio**

I eventually found this opportunity but cybersecurity where it kind of acts as this bridge. It's this way to take that passion and kind of connect it into this like real world positive impact.

And it really gave me a way to to like use those creative skills and just kind of make the world a little bit better, which I mean, to me, that's like a super important thing. ah It means a lot to me.

So really, when I discovered that, that's when it stopped being just a career. And it's a meaningful way for me to contribute to something bigger.

**Kerrin Mitchell**

Wow. I love that. Tim just got very excited too because his his family.

**Tim Sarrantonio**

Oh, I did. I mean, I love the direct correlation between artistic creativity and hacking. It is so fascinating.

**Kerrin Mitchell**

Yes. Go ahead. Mm hmm.

**Tim Sarrantonio**

I will ask a question that popped up kind of in my head organically here.

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

What do you think is the best representation of hacking in popular culture? Like what's an accurate representation of hacking?

**Chris Aurelio**

In popular culture.

**Kerrin Mitchell**

Very interesting question, Tim.

**Tim Sarrantonio**

It's not going to be like the movie Swordfish, right?

**Kerrin Mitchell**

Look at you. Off scripting. Crazy kid.

**Chris Aurelio**

No, no, no, nothing like that. Although I do really enjoy the movie Sneakers. ah So that one's pretty good.

**Tim Sarrantonio**

I was going to say, is it sneakers?

**Kerrin Mitchell**

Yeah.

**Tim Sarrantonio**

Yeah, yeah.

**Chris Aurelio**

um hey It's a little hard to say because I think the reality, at least the way that I experience it with my friends and colleagues, is not really portrayed in the media.

There's just sort of like a way that it happens that, quite honestly, you were to try to put it on the screen, it wouldn't be so fun to most people.

**Tim Sarrantonio**

Yeah.

**Chris Aurelio**

So ah it's long. It's a lot like thinking outside the box and just bringing creative energy to the table. And sometimes it's like you go to a conference with people, you're having a couple of drinks and just talking about weird things that lead you off onto these very interesting rabbit holes that then later kind of drive and inspire really fascinating work.

**Tim Sarrantonio**

So so that that does actually nicely dovetail into a question that that does connect to the topic, you know, because I can talk about Mr.

**Chris Aurelio**

Right.

**Tim Sarrantonio**

Robot all day, but that's not the purpose of this podcast. So...

**Chris Aurelio**

Sure.

**Kerrin Mitchell**

I love that.

**Tim Sarrantonio**

Because you actually bring up something very interesting here on going to conferences, connecting with people, right? I believe that about one third of all breaches in 2024 actually involved ransomware.

If that sounds, you know, on track or whatever the numbers are, there's always kind of a human element though that's in play here. I love reading about social engineering things, right?

Kind of overall, where,

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

When we get into some of the trends that you're seeing, maybe if you even want to, i don't want to steal your thunder, Kerrin, but like larger trends. And then how much of that, even though it is computer driven, is actually the vulnerabilities lie with like user error or things that are very controllable by the average person, like leaving their computer screen open, you know, where somebody can see certain information, for instance, that type of stuff.

**Kerrin Mitchell**

Yeah.

**Tim Sarrantonio**

So what are the bigger trends? And then where do the humans sit in that?

**Kerrin Mitchell**

Mm-hmm. Yeah.

**Chris Aurelio**

So I think what the trends kind of confirm is this thing that we've known for a long while, ah which is the most vulnerable.

**Kerrin Mitchell**

Everywhere.

**Chris Aurelio**

They don't really live in code. They live in behavior. So when you look at it, I think it's roughly 68% of breaches now involve this human factor.

And that could be something like clicking on a phishing link or reusing passwords or even just accidentally sending sensitive data to the wrong person because it doesn't have to be know malicious or intentional.

**Tim Sarrantonio**

Mm-hmm.

**Chris Aurelio**

And when you combine that with this fact that somewhere around 77% of breaches are starting with stolen credentials, um The thing that becomes clear is the front door to most of these attacks, it's being unlocked by the user.

and that's really not about blame, ah but we just need to recognize where it is we should be focusing. And I think this is where organizations really need to think of security training and security awareness, and not just as a checkbox, but really consider it a frontline defense.

If we invest in tools like MFA and single sign-on and password managers, um it's really gonna make it a lot harder for single human error to become this systemic breach. So that's... ah That's kind of the pattern that we're seeing and and the biggest defense that we have to it.

### **Kerrin Mitchell**

So when we look at things like philanthropy in the social sector, are there specific trends or things that you think are almost sector specific that you want to be able to highlight to folks to say, hey, in and above, obviously, procedural... you know, loopholes and mitigation around those sort of human aspects. Are there things that you're also seeing that come from us working in a social sector where we have very, very valuable data, very, very valuable missions um and very, very scary, like repercussions, right, for things going wrong?

### **Chris Aurelio**

Yeah, absolutely. I think in the social sector in particular, you have a lot of constrained resources when you have a lot of high regulatory obligations and you have a ton of surface area and it's not really just about protecting the data.

But about protecting the community and the trust that's been built. So there are a lot of these pieces that make it particularly challenging in social sectors.

And I think that attackers kind of realize this and they're looking for environments that are fairly constrained in resources. That kind of starts off in a very disadvantaged position.

But the the fortunate thing is it doesn't take a a really complex set of controls or environments to be able to to drive real effective impact and change.

We can start with the basics and really kind of

reinforce those things around access control and around vendor validation and around making sure that we have all of these necessary governance pieces in place and using the existing tools that folks already have.

So it doesn't require this additional investment.

### **Tim Sarrantonio**

I think that's a really important point because I want to talk about the speed and sophistication that is happening, especially as these folks get utilization of artificial intelligence and stuff like that.

On the individual giving side, because that's kind of my world that I've lived in for a very long time, for instance, fraud, credit card fraud in particular.

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

is out of control in terms of the attempts that we're seeing. I know this is happening with other providers as well. Basically, if you have an online donation form, it's going to get hit in a lot of different ways.

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

But, ah you know, especially from your perspective, because you're working with a different part of the social sector too, what are you seeing about the speed, the sophistication overall? How is it evolving, especially as we head into 2026?

What do we need to be on guard for?

**Chris Aurelio**

Oh, yeah, I mean, the velocity of attacks today is just staggering, honestly. um you know we used to think of cyber attacks as these long-term campaigns.

They were slow. They were stealthy. They required this deep technical expertise. And now we're seeing attacks moving from this initial access phase to full-scale impact in a matter of hours or even less.

And part of that is because you have these attackers that have automated much of the early stage work. But we have a lot of things like the rise of cybercrime as a service. Now you have anyone can purchase an exploit kit or or rent some ransomware, and it comes complete with customer support and payment portals.

And it really just professionalizes crime.

**Kerrin Mitchell**

Wow. Are you serious?

**Chris Aurelio**

Oh, absolutely.

**Kerrin Mitchell**

Oh my gosh.

**Tim Sarrantonio**

Cyber security sass.

**Kerrin Mitchell**

I mean, if I'm not, I'm like, of course it is.

**Tim Sarrantonio**

I wonder what the MQL rate is on that.

**Kerrin Mitchell**

How do those people sleep at night? Holy crap.

**Tim Sarrantonio**

Yeah.

**Kerrin Mitchell**

Anyway, I'm sorry.

**Tim Sarrantonio**

On their bed of, on their bed of Bitcoin.

**Kerrin Mitchell**

I guess I shouldn't be surprised. Sure.

**Chris Aurelio**

And the problem is compounded when you start layering in AI innovation. Right now attackers are becoming more convincing.

**Kerrin Mitchell**

And

**Chris Aurelio**

They can more easily impersonate executives and stakeholders and such. So it becomes a lot harder for employees to spot red flags.

**Kerrin Mitchell**

Wow.

**Chris Aurelio**

Um.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

And that's really where organizations need to start thinking about the entire life cycle of the threat. It can't just be about how to prevent an attack, but when something happens, how do you detect it early?

**Kerrin Mitchell**

Right.

**Chris Aurelio**

How do you contain it quickly? And how do you recover with minimal disruption?

**Kerrin Mitchell**

Right.

Yeah, continuity planning at that point is, it's inevitable as to, you will be hit at some point, so how do you handle it? Like admitting that it's not if, it's when. I think that's the thing that, you know, when you talked about, you had an obvious presentation recently for Fluxx, which was at our and or or quarterly state of Fluxx for the CEO presentation.

**Chris Aurelio**

Yeah.

**Kerrin Mitchell**

It was a lot about just the more digital operations, the remote work, all these sort of elements that add to this sort of larger target um for, you know, these lovely organized structures to hit that are absolutely a threat.

**Chris Aurelio**

Yep.

**Kerrin Mitchell**

And then basically having more targets means a larger risk perimeter of what you need to manage. What are some things that sort of come to your mind there about rethinking your digital awareness of that perimeter?

Like what are the things that you would recommend to folks as they think that through?

**Chris Aurelio**

Sure, well, the traditional idea of perimeter, honestly, it just doesn't hold up anymore. So in the past, you had these monolithic environments, you had a centralized network, and you had all these firewalls, and you had these very clear boundaries of what is the inside versus the outside.

But today, I mean, people are working from anywhere, and data lives in like a dozen saas platforms, and you've got AI tools that are integrated into workflows that didn't even exist a year ago.

So the boundaries have very clearly moved. At this point, we've got you know every every api every vendor that you're using, every endpoint is a potential risk vector.

And that goes into a whole digital sprawl that you'll hear people talking about, where the more distributed and the more integrated your tech stack is, the more discipline that you're going to need to again go back to these basics manage your access control and your vendor risk and just how you're kind of handling data um i think that that really like that reality it really forces us to kind of integrate security at every like layer whereas traditionally was something that we could kind of add on after the fact it isn't anymore

**Tim Sarrantonio**

Well, Chris, you're hitting on a really important point because it's not just a technical issue, right? it's ah It's an economic one. It's an operational one. It's a legal element, right?

**Chris Aurelio**

Sure.

**Tim Sarrantonio**

And so there's a lot of ways that you know we have to work together internally across organizations, across networks,

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

How can funders and grantees in particular work together to improve the resilience and the strength that we have protecting these really important data systems, these really important access points to what ultimately is powering the kindness and good in our society?

**Tim Sarrantonio**

So what do you think we could do about that? Simple question.

**Chris Aurelio**

Yeah, simple but an important question. Um, you know it's really about improving resilience, right? and it's important because resilience isn't something that any one group can achieve in isolation.

**Tim Sarrantonio**

Hmm.

**Chris Aurelio**

And this is where you know funders and grantees are part of the same digital ecosystem. And if one node is compromised, you know that impact, it could ripple out very quickly.

**Tim Sarrantonio**

Yeah.

**Chris Aurelio**

So the first step is to recognize that cybersecurity should be a part of capacity building and that funders can support grantees not only with financial resources, but with education and this kind of community building around best practices.

And that could look like a lot of different things. Um, you know they could include cybersecurity and grant making conversations, and not necessarily as a barrier, but seeing it as like a shared investment.

They could co-host awareness sessions where funders and grantees kind of like to learn together. There are a lot of options, but the key...

**Kerrin Mitchell**

You could even make it a part of the application process of understanding like we are a community that you know functions with a level of trust and here's how we'd like to make sure we're both showing up for each other.

**Chris Aurelio**

Yes.

**Kerrin Mitchell**

So yeah, it's like embracing it more than just another variable.

**Tim Sarrantonio**

Yeah. It's part of the social contract.

**Kerrin Mitchell**

It's part of the contract. The same way they're saying here's what the impact is, here's what the finances are, here's where a risk is, here's where you know we're mitigating for security you know concerns.

**Chris Aurelio**

Absolutely.

**Tim Sarrantonio**

Mm.

**Chris Aurelio**

Yeah, the key is whatever they decide to do, just approach it collaboratively.

**Tim Sarrantonio**

Mm.

**Chris Aurelio**

Right. They want to reduce friction by bringing security into the systems that both sides already use and just make it a team effort. So honestly, I think I was going to say, ah the more we can normalize security as a shared goal, I think the more resilient we all become.

**Kerrin Mitchell**

Yeah, I mean, I think, oh, sorry, go ahead.

And when we talk about sort of the main pillars of an approach that we would say, okay, let's deploy this. Let's talk about this. You know, obviously you've talked in the past. I've heard you talk about this like awareness, automation, and audibility. What are the types of things you would say here are the pillars to really look at as we look to bring those into like our operations and strategy, whether be grant maker, grant seeker.

How do you, what are some of your suggestions, if you will, of those things that they should be thinking about. And then maybe some tips to tips and tricks of things that you saw. And I'll, I'll let that be the next question, but I want to make sure, you know, what are the main pillars that you're looking at when you're talking about this?

**Chris Aurelio**

Well, I think that that trio is actually really important because that's how we operate and operationalize trust.

Yeah, that trio specifically is actually really important because that is how we operationalize trust. Awareness really ensures that people know how to spot risks and how to respond appropriately. The automation aspects, they're ensuring that we have the right protections that are applied consistently, um even when people are busy or distracted.

And that auditability, you know, gives organizations and customers the ability to verify that all the controls that they're using are actually working. So when we're investing in those pieces you know across both internal operations and the product, um it's really helping to to have um to elevate everything.

**Tim Sarrantonio**

Yeah, I think like where that kind of leads me is the practicalities here. And it would be interesting to hear from your perspective. I'm going to kind of ask two things because first you've mentioned some simple steps that people can take. Most people don't have a 20 person IT team, right?

**Chris Aurelio**

Sure.

**Tim Sarrantonio**

97% of nonprofits are under \$5 million. bucks Most of them are under \$1 million. dollars I've lived with. I've experienced this. I get the emails in my inbox from people getting absolutely spammed.

And then they send the email out that says, that wasn't me. You know, please disregard that.

**Chris Aurelio**

Right.

**Tim Sarrantonio**

That happens almost every other day just for my work email. And so there's things that people can do on their end. And I'd love to hear your perspective. But I actually would love to hear on the tech side, what are things that vendors could do to also make this easier for the average nonprofit or funder as well? Like what are stuff that you're interested in helping make it easy for this to happen, to put that security in?

**Chris Aurelio**

Absolutely. and you know, the good news is that security isn't really about complexity, ah but it is about consistency. So the tips that I generally like to reinforce for organizations of any size um start with turning on MFA everywhere you can. I will say this all the time.

I cannot say it enough, especially for things like email and cloud apps and just anything with sensitive data. Definitely turn on MFA. A second tip, encourage staff to use a password manager.

It is very easy for folks to want to reuse passwords, but they should not do it ever. You need to have unique passwords everywhere. just becomes too much for folks to remember. And a password manager is a really good low friction way to just keep good password hygiene.

A third thing, sticking to the least privilege. That's also a really, really easy but very high impact item. If you need to request access to something, only request what you need to do your job.

And when you don't need it anymore, let it go. you know If you're managing systems or you're managing teams, try to make access reviews a regular habit and just think of it a little bit like spring cleaning.

If there's a permission that doesn't serve a clear purpose, it probably shouldn't be there. Just get rid of it. And the last thing that I like to tell folks, which is easy to forget, is train your team, right?

Because they can't drive impact if they don't understand what it is that they're supposed to be doing or how it is that they're supposed to do it.

So training the team becomes really important and not to do that with fear, but use real world examples and kind of you know show folks the things that are expected, right? How do you spot fishing or,

How do you report an incident or just, you know, in general, how, how do they drive impact in their roles?

**Tim Sarrantonio**

If you get in text from the CEO asking you to go buy gift cards, it is not a real thing, right?

**Kerrin Mitchell**

Right.

**Chris Aurelio**

Yes.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

Don't do it.

**Tim Sarrantonio**

And that's where vendors also come in to kind of help identify or or I know that you can communicate at scale, hey, we're seeing these types of things.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

Absolutely.

**Kerrin Mitchell**

And if I do think that this is things that someone likes, well, I don't know how to educate people on this. And this is actually where Chris has done an awesome job for our internal operations. We have a number of things that we actually utilize training. There's like these goofy, albeit not goofy, but these monthly things that Chris has us do that are these security awareness things.

And they're actually mildly entertaining. And they're like these little videos that every single person at Fluxx has to watch and answer these questions. And it's a service we pay for. And I

don't think it's that expensive. But it makes it take that training aspect off of, say, the head of operations who might be like, how would I know what to train on?

**Kerrin Mitchell**

This is actually, and I don't know what it's if you want to give it a plug for what it's called, but it's like there are services that do this. They are awesome.

**Tim Sarrantonio**

Mm-hmm.

**Kerrin Mitchell**

Yes, as an employee, some of them make me giggle because they're ridiculous. But for the most part, I'm also paying attention. I think it's interesting. And we also have things like security channels that Chris is setting up inside of our Slack that gives us the ability to sort of convey, you know, key learnings, key articles, things like that. So Chris, I don't know if there's anything that you think you really like. I imagine the videos that we get to watch every month are up there for you. But it really takes a lot of that burden off of Chris too to have to do some of the education because there are incredible opportunities to use content that is incredibly up to date and entertainment forward.

**Chris Aurelio**

Yeah, absolutely. I mean, there are a ton of organizations out there that can be partnered with to be able to help with the security training and awareness.

**Kerrin Mitchell**

Yeah.

**Chris Aurelio**

So there really is no lack of options.

**Kerrin Mitchell**

Yeah.

**Tim Sarrantonio**

Can I give a plug for one that I just worked with recently?

**Chris Aurelio**

Um.

**Kerrin Mitchell**

Yeah.

**Tim Sarrantonio**

It was the Center for Cyber Safety and Education.

**Kerrin Mitchell**

Do it. Cool.

**Tim Sarrantonio**

And they're an actual nonprofit that focuses on nonprofits themselves.

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

We just had Holly from their team present at Generosity Exchange, kind of the Neon One conference.

**Kerrin Mitchell**

Oh, killer.

**Tim Sarrantonio**

Um.

**Kerrin Mitchell**

Nice.

**Tim Sarrantonio**

And that was kind of like some of the basics that you're talking about here too.

**Chris Aurelio**

Excellent.

**Tim Sarrantonio**

But I know there's a lot of different options.

**Kerrin Mitchell**

Yeah, I mean, it sounds good, but totally.

**Tim Sarrantonio**

There's a lot of stuff out there.

**Chris Aurelio**

There are, and it's really just about getting people involved. You can do so many different things.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

I'm not going to get too perspective on the actual method you choose or the company that you partner with, as long as you're just trying to take little steps. And then just kind of evaluate, see how your teams are receptive to the information.

**Kerrin Mitchell**

Mm-hmm.

**Chris Aurelio**

Not every solution is going to work right out of the box for every environment. So just you try it out and you see what doesn't work and you modify it and make it better each time.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

Thanks.

**Kerrin Mitchell**

Killer. All right. So we ah unfortunately do have to wrap up soon, but I'm wondering when we look at the future and there's a lot of places again, where things can look like, Oh my gosh, it's only getting worse.

It's only picking up speed. It's only getting more pervasive and our risk perimeters are spiraling into a new realm. What gives you hope? What are the things that you're most excited about or perhaps structures that are coming up where you say there's some really interesting work that's happening here that gives me hope for managing a lot of this volume, right?

How do we meet that moment?

**Chris Aurelio**

Yeah, I mean, the biggest thing that gives me hope is this growing sense of a shared purpose, right? So more and more, I see people coming together, not just to protect their own systems, but just to strengthen the overall community.

And there's a real shift that's happening where cybersecurity is no longer seen as just this blocker or a burden to organizations, but as a key enabler of mission success. And to me, that's really encouraging.

I also see a lot of real momentum happening where we see things like tools using more secure defaults and more open conversations around risk and just more collaboration across organizational units that just used to operate in silos. So all of these things I think are really good signs of the direction that we're moving in, just having more transparency and more accountability and driving more impact.

Because those are all things that are the foundation of a strong security program. And I think that when we bring that mindset into how we're designing systems and how we're partnering with others, then it starts becoming a part of how we lead.

**Kerrin Mitchell**

Yeah, it's a fabric. Yeah, amazing. um Tim, anything else you wanted to cover? Or Chris, anything that we wish we had asked you that we did not ask you?

**Chris Aurelio**

The one thing that I think about is what is a question that other people should be asking? And I think the one thing I'd like to see more people ask is how do they build resilience and not just respond defensively to threats?

**Kerrin Mitchell**

Right.

**Chris Aurelio**

There are, again, a lot of ways that you can answer that. And I think just asking that question is important because going through the exercise is going to cascade with a lot of high impact items. So if people just start asking that question and practicing that exercise more, I think I think a lot of good things will come out of it.

**Tim Sarrantonio**

Well, and I think that connecting it back to the fact that you discovered this because of art makes that question even more potent.

For real, it's a very philosophical question.

**Kerrin Mitchell**

Yeah. Yeah.

**Chris Aurelio**

Yeah.

**Tim Sarrantonio**

And so I think that it's funny for us to end on this game, Kerrin, because it's true truths and lies. So basically, like, you're trying to pen test us. And so, Kerrin, do you want to explain kind of how the rules on this work?

**Kerrin Mitchell**

Yeah.

You know two truths and a lie, right, Chris?

**Chris Aurelio**

Yeah.

**Kerrin Mitchell**

Okay.

**Tim Sarrantonio**

So..

**Kerrin Mitchell**

Give it to us. Give us two truths and a lie. going to guess which one is your lie.

**Tim Sarrantonio**

We're going to guess, and we don't have to have the same one, but we tend to to try to align.

**Kerrin Mitchell**

You can take a second, too. We realize this. We might have sprung this on you. So if you need a moment, you take it. Okay.

**Chris Aurelio**

All right, two truths and a lie.

Number one, security is about consistency. Number two, and MFA is important, but it's complex to set up. And number three, good security can happen even with small teams and resources.

**Tim Sarrantonio**

I love how this is the first time we've had somebody turn it in on their own topic.

**Kerrin Mitchell**

I love it. I love it.

**Tim Sarrantonio**

I love it.

**Kerrin Mitchell**

So Chris, that actually is for everyone, always says two lies about themselves.

**Tim Sarrantonio**

It's like a quiz about themselves.

**Kerrin Mitchell**

And I kind of love that. Yeah.

**Tim Sarrantonio**

And it's fine. Like we've loved it. But now I have to actually think.

**Kerrin Mitchell**

We don't care. We love it. But I love it. This is a content based one. The

**Tim Sarrantonio**

It is. It's great.

**Chris Aurelio**

I thought about awareness.

**Tim Sarrantonio**

I think it's the second one.

**Kerrin Mitchell**

The answer is two. It's two.

**Tim Sarrantonio**

I think it's number two.

**Kerrin Mitchell**

It's easy.

**Tim Sarrantonio**

I think it's two.

**Kerrin Mitchell**

It's two.

**Chris Aurelio**

That's right. MFA is not complex to set up.

**Kerrin Mitchell**

Yay, Tim.

**Chris Aurelio**

It is important, but it is easy to do.

**Kerrin Mitchell**

We learned stuff. I like this new opening.

**Chris Aurelio**

Someone is at the MFA.

**Tim Sarrantonio**

We might have to flip it.

**Kerrin Mitchell**

Our aperture of this game just opened. Chris, thank you so much for joining us today.

**Tim Sarrantonio**

Yeah. Yeah.

**Kerrin Mitchell**

Chris, thank you so much for joining us today on the podcast. Of course, invaluable information is shared with not just our listeners, but Tim and I always learn stuff too. So we are so appreciative of you just generally for joining us, but also at Fluxx, we are so lucky to have you, of course.

**Chris Aurelio**

Yeah, thanks for having me.

**Kerrin Mitchell**

Thank you so much, friend.

**Chris Aurelio**

I appreciate it.

**Kerrin Mitchell**

Right.

**Chris Aurelio**

Thank you for giving me the opportunity to be here and share this information.