The Cybersecurity Readiness Podcast Series

Episode Title	Passwordless Authentication: Myths and Realities
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Ori Eisen, Founder and CEO of Trusona
Summary Pitch	Driven by a mission and passion to fight online crime, Ori Eisen, Founder and CEO of Trusona, explains the fundamentals of passwordless authentication and why it is a superior and simpler way of securing access. He also dispels several myths and addresses potential adoption hurdles, ranging from incompatibility with legacy applications to transition costs, regulatory compliance, privacy concerns, and more. Ori offers some valuable tips and recommendations to protect individuals from becoming victims of hacking. Finally, he shares some hilarious jokes at the end.
Time Stamps	02:40 -- If you could give us a little bit of a primer on what is passwordless authentication. 05:10 -- So can you help dispel some of the myths around passwordless authentication? 09:10 -- What would be some factors that could influence an organizational decision of adopting a particular method? 11:32 -- So how are users being authenticated? And what about that information that is being used to authenticate individuals? How is that

	secure? And if that falls in the hands of the wrong, folks, isn't that concerning? 14:44 -- So when I was doing my research on this topic, and I was trying to learn about the pros and cons of passwordless authentication, something that came up was incompatibility with legacy applications. Could you speak to that? 16:12 -- Okay, now, you mentioned FIDO. What is FIDO? 17:32 -- So it seems like we don't have to choose between convenience or security, we can have the best of both worlds, right? 19:07 -- Now the solution sounds great. And we need to move in that direction. What about the cost aspect of it? I've read that the cost implications can be significant. Is there any truth to that? 21:04 -- What about the regulation aspect of it, I was reading somewhere that -- regulations require clear information on data storage, considering the sensitive nature of passwordless data when it isn't stored appropriately, there could be a lot of issues, would you? How would you react to this statement? 23:46 -- What about privacy concerns? You think users, you know, how would you alleviate privacy concerns amongst users? 25:29 -- What is the relationship between passwordless authentication, multi-factor authentication, and mobile multi-factor authentication? 28:17 -- Multi-factor authentication becomes much stronger and effective if you were to go passwordless. Correct? 29:09 -- Well, let's talk about the bad guys. And let's talk about your motivation, what got you doing, what you're doing, and all the great things you've been doing and trying to reduce or fight online crime. 30:59 -- What tips or recommendations would you have to anyone from protecting themselves from different types of attacks?

	34:15 -- So, Ori, what are your thoughts about a strong password and how best to store passwords? 37:24 -- Ori, share with us that VC joke that I heard in one of your other podcasts the other day. I think our listeners would love to hear that joke. 39:27 -- What's the other joke? 40:13 -- Any final words to wrap up this session?
Memorable Ori Eisen Quotes/Statements	"Maybe passwords are not the most secure thing. And our parents are not security experts we should trust with creating long and complicated ends, passwords. So the whole idea of getting passwordless is to remove this factor, which as you probably know, contributes to 81% of all the data we see lost out there and just do away with it. Because the technology to do it is already in our pockets." "The first thing to know is that passwordless authentication does not use static passwords that users pick. So that's the first thing to know. So obviously, you can ask, Well, what does it use? It uses the very same architecture and technology we already have used for e-commerce in the form of HTTPS certificates, and public and private keys." "Putting your passwords into a password vault does not eliminate them. And if you were to inspect with Wireshark or Ethereal, the connectivity between you and the server, you'll see that the password vault only saves you from remembering it, but it's still on the wire. So if you have malware or anything like a Man-In-The-Middle, you are still revealing your credentials." "It's not about money anymore. The delta between going passwordless or not, on many of the systems is just your sheer will. That's it." "So I'm a proponent of not changing the taboo, not changing the security behavior, because then you have something to overcome. Let's make it easy, ubiquitous, and democratize it."

	"I hope today if I say fax me your resume, you'll think that's crazy. I hope that using a password will be just as crazy a few years from now."