The Cybersecurity Readiness Podcast Series

Episode Title	Reducing the Risk of Social Engineering to Exploit IT Help Desk
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guests	Mike Manrod, the Chief Information Security Officer (CISO) of Grand Canyon Education Ori Eisen, Founder and CEO of Trusona
Summary Pitch	In this episode, Mike Manrod, the Chief Information Security Officer (CISO) of Grand Canyon Education, and Ori Eisen, the Founder and CEO of Trusona, joined me to discuss how best to reduce the risks of social engineering attacks on IT support and help desk personnel. This episode was motivated by the major cyber attack that brought MGM Resorts International's operations to a screeching halt. It was a social engineering attack where the attackers gained super administrator privileges by providing the MGM Help Desk with basic employee information. **Action Items and Discussion Highlights** • "Bypassing the human verification is something super critical we need to address. It's something we can't afford to wait on, and it's low-hanging fruit." • Implement a driver's license validation solution to authenticate callers to the IT help desk. • Explore expanding the use of identity verification technologies beyond the IT help desk, such as for wire transfers and other high-risk financial transactions. • Adopt a layered approach to establishing a robust defense. "You need a good tech stack, user entity behavior analytics,

	conditional access policies, MFA, and security awareness training." • Educate IT support staff on identifying potential social engineering attempts, even when the caller appears to be using advanced techniques like voice cloning. • Implement a policy instructing employees to hang up and call back when they receive requests for sensitive information or transactions. • Stay vigilant and continue to explore new solutions to combat the evolving threat of social engineering attacks.
Time Stamps	00:02 -- Introduction 02:45 -- Mike Manrod's professional highlights 03:38 -- Ori Eisen's professional highlights 06:36 -- Why is Mike Manrod so passionate about this discussion topic? 08:45 -- Breaching MFA 13:25 -- Securing the Organization from Human Vulnerabilities 17:57 -- Defense-in-Depth and People-Process-Technology 19:44 -- Technology underlying authentication 22:40 -- Seamless adoption of authentication technology 26:15 -- Evolution of authentication technologies 30:02 -- What advice would you have for practitioners like you who are on the fence about investing in such technologies? 31:10 -- Closing Thoughts

Memorable Mike Manrod Quotes/Statements	"Multifactor authentication (MFA) carried us a long way, but now that it's everywhere, it naturally creates a cyber evolutionary force, driving adversaries to have to solve it." "I think the future is that of a layered approach. No one solution solves the whole problem. You need a good tech stack; You need user entity behavior analytics; You need conditional access policies; You need MFA; You need security awareness training." "You can't simply rely on five verification questions that anybody could guess." "We were really excited about the driver's license validation aspect, you know, let's take a trusted authority like a driver's license bureau. Let's take a trusted identification with multiple attributes that can be verified and then put it on a clock so that if somebody somehow tries to socially engineer those chains, we detect and report on that too." "Bypassing the human verification is something super critical we need to get on top of, and it's something we can't afford to wait on, and it's low-hanging fruit."

Memorable Ori Eisen Quotes/Statements	"If everybody has MFA, no one has MFA." "It is called push fatigue, and it comes when messages, emails, and alerts are constantly being pushed down to people, and they are having to react. They just click "Okay" out of habit, and that's how access credentials get shared." "Now you're in a social engineering battle that is all about identity, nothing about authentication anymore. I think that is the new wave of attacks we're going to see because they work, and they bypass the whole need to really be a supercomputer engineer." "You don't need to be a super hacker with code. You can be a super hacker with social engineering and bring the whole network down. "A very large airline has confided in us that their CEO was on CNN giving an interview. The cyber gang sampled his voice from that interview to call an AI modulator into the IT Help Desk and belligerently scream at them to reset the password. They had this as a recording, and they played it to the CEO, who said, I would not be able to know that it wasn't me. It is that good."