The Cybersecurity Readiness Podcast Series

Episode Title	Stopping Deepfake Threats: Protecting Organizations Through Identity Verification
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Aaron Painter, CEO at Nametag
Summary Pitch	In this episode, Aaron Painter, CEO at Nametag, joins me in discussing the Deepfake fraud phenomenon and how organizations and individuals should protect themselves from such scams. A recent study conducted by finance software provider Medius finds that over 53% of businesses in the U.S. and U.K. have been targets of financial scams powered by "deepfake" technology, with 43% falling victim to such attacks. 85% of the finance professionals polled view such scams as an "existential" threat to their organization's financial security. In the United States, families lose an average of $11,000 in each fake kidnapping scam. According to data from the Federal Trade Commission, Americans lost $2.6 billion last year in imposter scams. **Action Items and Discussion Highlights** ▪ Assess where deepfakes could be used to target the organization and implement a multi-layered defense strategy. ▪ Injection attacks and presentation attacks are the two keyways that deepfakes are deployed. If you're using things like modern mobile phones to prevent against injection attacks thanks to cryptography,

	then you've shut down one of the main ways that people are using injection attacks. If you're able to use the three-dimensional face ID camera, you have an incredibly sophisticated tool to prevent against presentation attacks. ▪ Deploy robust multi-factor authentication methods beyond SMS, such as authenticator apps. ▪ Establish strong protocols for verifying user identities during account lockouts and new hires/onboarding. ▪ Explore using cryptography, biometrics, and advanced device-based checks to prevent deepfake injection and presentation attacks. ▪ Provide employee awareness training on deepfake threats and best practices for verifying digital identities.
Time Stamps	00:02 – Introduction 02:28 – Guest Speaker's professional highlights 04:40 – Deepfake Phenomenon Overview 06:44 – Examples of Deepfake Frauds 10:46 – Human Vulnerability to Deepfake Scams 14:45 – Solutions and Remedies 19:08 – Effective adoption and use of anti-Deepfake technologies 27:43 – Advice on how individuals can protect themselves from Deepfake scams 30:34 – Closing Thoughts

Memorable Aaron Painter Quotes/Statements	"The world of identity verification is so fundamental in protecting our digital lives, and it just needs to be done differently." "We as humans have learned to trust what we see and what we hear; and so as interactions have moved to these digital platforms, whether it's video conferencing teams and Zoom or phone calls, FaceTime, you name it, we assume that when we see someone and we hear them interact and we hear their voice, that it's something we trust and that we automatically can trust it." "The rise of these new generative AI tools has given superpowers to bad actors, and they are now able to impersonate us in an incredibly easy way across a variety of different scenarios and use cases." "Researchers have found that with three seconds of someone's audio clip, they can create a voice deepfake of you." "The process of getting around MFA today has become too easy." "Increasingly, we're seeing this incredible risk of impersonation attacks happening at this moment of hiring or onboarding, and this has really become the number one concern, particularly in the last few months" "Mobile phones give us the platforms to do this multimodal approach of deepfake defense; Web browsers do not." "People understanding more about these deepfake threats allows them to be better protected."