

Conan O'Brien Teams Up With Adaptive Security To Fight AI Threats with Laughs

Adaptive Security and Conan O'Brien are turning comedy into a defense against deepfakes, voice cloning and AI impersonation through a new cybersecurity awareness training series

NEW YORK, June 9, 2026 /PRNewswire/ -- As organizations across every industry race to get ahead of AI-powered attacks, Adaptive Security is adding an unlikely weapon to the arsenal. The company today announced a 15-video cybersecurity awareness training series starring Conan O'Brien and filmed in Los Angeles. The series uses O'Brien's signature absurdist humor to teach employees how to recognize and stop modern threats, from AI-generated voice calls to deepfake video and hyper-targeted phishing. The training series is immediately available to Adaptive's current enterprise customers and comes included for any organization that joins the platform. Organizations interested in accessing the training series can visit adaptivesecurity.com/conan.



The Conan training videos cover two categories of security awareness content. The first addresses the AI-powered attacks driving the fastest growth in incidents today, including deepfakes, voice cloning, and AI impersonation. The second covers the foundational topics every corporate security awareness program requires, including email and SMS phishing, QR code scams, password vulnerabilities, physical security and remote work risks. O'Brien's

team co-wrote the scripts with Adaptive and improvised on set, bringing his signature smart and silly comedic instincts to each topic.

Security awareness training has had an engagement problem for years, a fact that will not surprise anyone who has sat through it. Most employees click through standard compliance modules without retaining the content. Organizations spend billions annually on training programs that employees tend to forget before their next login. And the tactics are evolving faster than the training designed to address it. In 2025, Adaptive reported that more than half of its enterprise customer conversations included firsthand accounts of deepfake attacks inside their organizations. Deloitte projects that AI-facilitated fraud losses in the U.S. will grow from \$12.3 billion in 2023 to \$40 billion by 2027.

"Voice phishing, deepfake personas and AI-generated impersonation are hitting companies every week, and most training programs were built years before those attacks existed. We wanted to build something personal and engaging, something employees would actually look forward to," said Brian Long, CEO and co-founder of Adaptive Security.

Conan O'Brien spent decades as a late-night television host on NBC and TBS before building a second career in podcasting through Team Coco. His comedy turns out to be an unusually

effective defense. AI-powered attacks succeed by manufacturing urgency and panic. O'Brien's humor, rooted in absurdism and committed deadpan, trains employees to slow down and look twice before they act.



"He made every script funnier by bringing his enthusiasm to every take, and left us feeling like we made something truly special," Long said. "We are incredibly lucky to have him as a partner in this."

"I teamed up with Adaptive Security just to figure out what these kids are up to. Turns out it's pretty cool," O'Brien said.

Why Security Awareness Training Will Never Be the Same

Each of the 15 training modules opens with a comedic O'Brien introduction that frames the cybersecurity threat in a way employees are unlikely to forget. Adaptive's existing instructional material, interactive elements and knowledge checks follow each introduction without modification. For each module, customers see

two versions displayed side by side in their content library, a standard version and a Conan version, giving security teams full control over what they assign to employees.

Deepfakes, Voice Cloning, and Conan

O'Brien's voice and likeness are themselves relevant to the subject matter. The same AI tools that power modern deepfake attacks can clone his voice and face with the kind of ease that would have seemed far-fetched when he started his television career. Adaptive estimates that up to 60% of employees fail AI-powered attack simulations without prior training.

"AI puts sophisticated attack tools in anyone's hands," Long said. "We needed training employees would actually watch and actually remember. That was the whole idea."

About Adaptive Security

Adaptive Security, co-founded by Brian Long and Andrew Jones, is the leading provider of AI-powered social engineering prevention solutions. The company defends more than 1,000 enterprise customers against AI-powered attacks including deepfakes, voice cloning, advanced phishing and social engineering. The platform includes security awareness training, phishing simulations, phish triage, email security, AI governance and risk scoring. Adaptive Security has raised over \$140MM from investors like Bain Capital Ventures, NVentures (NVIDIA's venture capital arm), OpenAI Startup Fund, Andreessen Horowitz (a16z), Abstract Ventures, Capital One Ventures and Citi Ventures.

For more information, visit www.adaptivesecurity.com.

Media Contact

Joshua Thompson
josh@adaptivesecurity.com
Cell 716-864-4429
www.adaptivesecurity.com