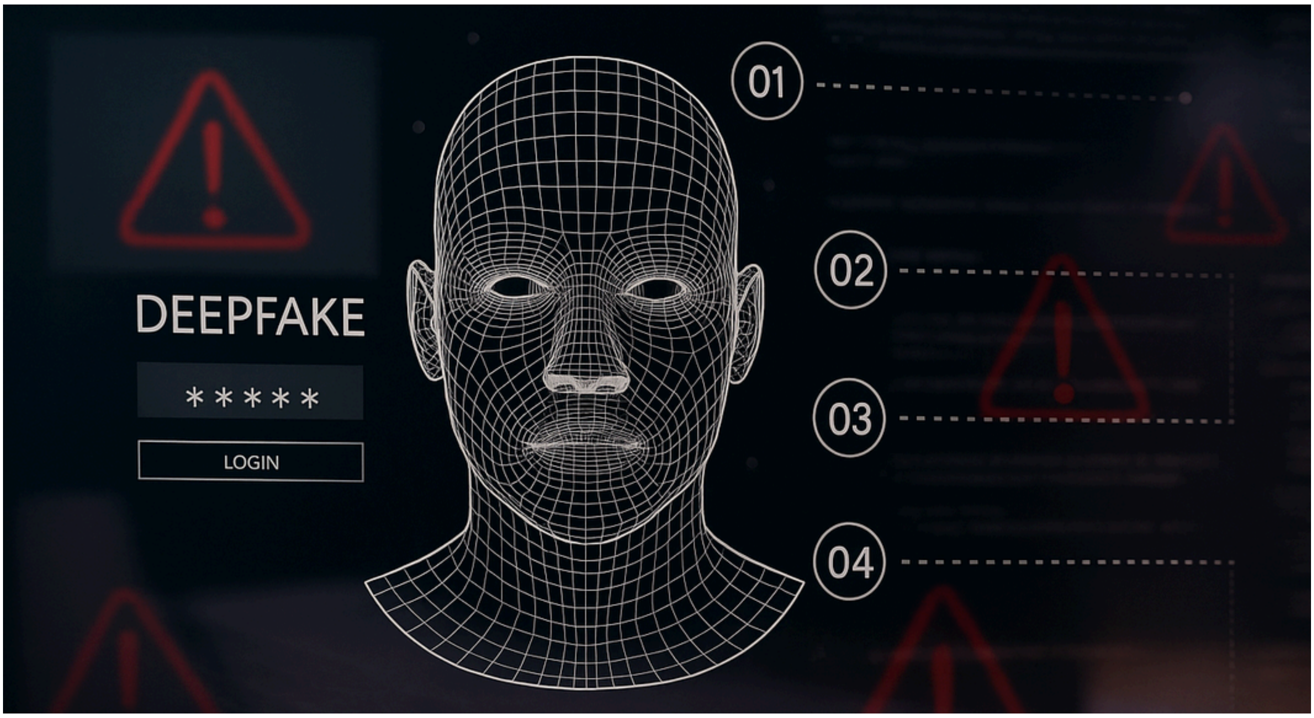
MAY 2025

McLaren Strategic Solutions

Newsletter

Rising Threat of Deepfakes in Enterprises



At McLaren Strategic Solutions, we recognize that deepfake technology is no longer a distant threat, it poses a real and growing risk to both our organization and the clients we support. As a technology-driven company entrusted with sensitive communications, high-stakes client engagements, and executive-level interactions, we are equally susceptible to deepfake-driven impersonation and manipulation.

Consider the case of a British engineering firm that was conned out of $25 million through a deepfake video call with what appeared to be their CFO. In another attempt, cybercriminals posed as the CEO of the world’s largest ad agency during a Microsoft Teams meeting, with cloned voices and doctored video. In yet another instance, a UK-based company fell victim to a voice-based deepfake impersonating an executive, resulting in a $243,000 loss.

These incidents are no longer theoretical, they’re real, they’re happening, and they’re targeting enterprises. It's time to re-evaluate how we verify identity in a world where seeing and hearing is no longer believing.

Deepfake - An Overview

Artificial Intelligence (AI) can now generate highly realistic images, audio, and video that look and sound completely authentic. These capabilities have many positive applications—advertising teams use AI-generated visuals in campaigns, film studios de-age actors in blockbuster movies, and educators create engaging video lessons using this technology.

However, when AI is used to deliberately create fake content to mislead or deceive, it's called a deepfake—a term that combines "deep learning" (a branch of AI) and "fake." The most harmful deepfakes are those that mimic real people, making them appear to say or do things they never actually did. Cybercriminals, for instance, can create fake videos of public figures committing crimes or spread false information through manipulated media. In more targeted attacks, they may clone someone's voice to impersonate them in phone calls, tricking friends, family, or coworkers. What makes deepfakes particularly dangerous is their realism, anyone's face or voice can be convincingly replicated, blurring the line between real and fake in ways that are hard to detect.

As a McLaren team member, it is vital we stay updated on these technologies, not only to protect our internal operations but to better support clients relying on us to anticipate and mitigate AI-driven risks.

Common Types of Deepfakes

IMAGE DEEPFAKES

Image deepfakes involve AI-generated photos - either of people who don't exist or of real individuals depicted in situations that never happened. These manipulated images are often used to tarnish reputations, evoke strong emotions, or fuel misinformation campaigns.

AUDIO DEEPFAKES

Audio deepfakes use AI to clone someone's voice, producing convincing fake recordings or phone calls. By extracting voice samples from public sources like podcasts or YouTube, attackers can replicate a person's speech patterns with startling accuracy.

VIDEO DEEPFAKES

Video deepfakes alter both a person's voice and facial expressions. These can be pre-recorded or generated in real time, such as during virtual meetings, making it appear as if someone said or did something they never actually did.

TEXT-BASED DEEPFAKES

AI can now generate realistic messages, emails, or chat conversations that mimic an individual's writing style and tone. These text-based deepfakes can be used in phishing attacks or business email compromise (BEC) schemes, where attackers impersonate executives or partners to manipulate recipients.

How to Detect Deepfakes

Trying to spot deepfakes by looking for visual or audio errors is no longer effective. As AI technology evolves, both the fakes and the people using them are becoming increasingly convincing. Instead of scanning for flaws, focus on context - does what you're seeing or hearing actually make sense?

Trust Your Instincts

If something feels off, it probably is. Is the message overly urgent or out of character? Does the person seem unusually pushy? Pause and double-check before acting.

Be Wary of Emotional Pressure

Deepfake attacks often rely on urgency, panic, or guilt to pressure victims into making rash decisions. Any communication triggering a strong emotional response should be a red flag.

Use a Secondary Verification Method

If something seems suspicious, verify it through a trusted channels - call, email, or message the person via a known contact method.

Set Up a Code Word or Phrase

Establish a code word within your team or organization to authenticate urgent requests. If someone cannot provide the code, it's a warning sign.

Conclusion

Deepfakes are becoming a real threat to how organizations work, communicate, and make decisions. At McLaren, our role is to stay ahead of these evolving tactics, not just to protect ourselves, but to empower our clients with actionable strategies.

Let's continue to lead by example, questioning unusual requests, reinforcing secure practices, and fostering trust in an age where digital deception is becoming harder to detect.

Remember: if something feels off, it probably is. Trust your instincts, use trusted channels to confirm, and don't hesitate to speak up.

Together, we can stay one step ahead!