Deepfakes Are on the Rise — Will They Change How Businesses Verify Their Users?

Opinions expressed by Entrepreneur contributors are their own.

You know how you can’t do anything these days without proving who you are? Whether opening a bank account or just hopping onto a car-sharing service. With online identity verification becoming more integrated into daily life, fraudsters have become more interested in outsmarting the system.

Criminals are investing more money and effort to overcome security solutions. Their ultimate weapon is deepfakes — impersonating real people using artificial intelligence (AI) techniques. Now, the multi-million question is: Can organizations effectively employ AI to combat fraudsters with their tools?

According to a Regula identity verification report, a whopping one-third of global businesses have already fallen victim to deepfake fraud, with fraudulent activities involving deepfake voice and video posing significant threats to the Banking sector.

For instance, fraudsters can easily pretend to be you to get access to your bank account. Stateside, almost half of the companies surveyed confessed to being targeted with the voice deepfakes last year, beating the global average of 29%. It’s like a blockbuster heist but in the digital realm.

And as AI technology for creating deepfakes becomes more accessible, the risk of businesses being affected only increases. That poses a question: Should the identity verification process be adjusted?

Related: Deepfake Scams Are Becoming So Sophisticated, They Could Start Impersonating Your Boss And Coworkers

Endless race

Luckily, we're not at the "Terminator" stage yet. Right now, most deepfakes are still detectable – either by eagle-eyed humans or AI technologies that have already been integrated into ID verification solutions for quite some time. But don't let your guard down. Deepfake threats are evolving quickly – we are already on the edge of witnessing persuasive samples that can scarcely arouse any suspicion, even upon deliberate scrutiny.

The good news is that the AI, the superhero we've enlisted to fight against good old "handmade" identity fraud, is now being trained to spot fake stuff created by its fellow AI buddies. How does it manage this magic? First of all, AI models don't work in a vacuum; human-fed data and clever algorithms shape them. Researchers can develop AI-powered tools to remove the bad guys of synthetic fraud and deepfakes.

The core idea of this protective technology is to be on the lookout for anything fishy or inconsistent while doing those ID liveness checks and "selfie" sessions (where you snap a live pic or video with your ID). An AI-powered identity verification solution becomes the digital Sherlock Holmes. It can detect both changes that occur over time, like shifts in lighting or movement, and sneaky changes within the image itself – like tricky copy-pasting or image stitching.

Fortunately, AI-generated fraud still has some blind spots, and organizations should leverage those weak points.

Deepfakes, for instance, often fail to capture shadows correctly and have odd backgrounds. Fake documents typically lack optically variable security elements and would fail to project-specific images at certain angles.

Another key challenge criminals face is that many AI models are primarily trained using static face images, mainly because those are more readily available online. These models struggle to deliver realism in liveness “3D” video sessions, where individuals must turn their heads.

One more vulnerability organizations can use is the difficulty in manipulating documents for authentication compared to attempting to use a fake face (or to “swap a face”) during a liveness session. This is because criminals typically have access only to one-dimensional ID scans. Moreover, modern IDs often incorporate dynamic security features that are visible only when the documents are in motion. The industry is constantly innovating in this area, making it nearly impossible to create convincing fake documents that can pass a capture session with liveness validation, where the documents must be rotated at different angles. Hence, requiring physical IDs for a liveness check can significantly boost an organization’s security.

While the AI training for ID verification solutions keeps evolving, it’s essentially a constant cat-and-mouse game with fraudsters, and the results are often unpredictable. It is even more intriguing that criminals are also training AI to outsmart enhanced AI detection, creating a continuous cycle of detection and evasion.

Take age verification, for example. Fraudsters can employ masks and filters that make people appear older during a liveness test. In response to such tactics, researchers are pushed to identify fresh cues or signs of manipulated media and train their systems to spot them. It’s a back-and-forth battle that keeps going, with each side trying to outsmart the

other.

Related: The Deepfake Threat is Real. Here Are 3 Ways to Protect Your Business

Maximum level of security

In light of all we've explored thus far, the question looms: What steps should we take?

First, to achieve the highest level of security in ID verification, toss out the old playbook and embrace a liveness-centric approach for identity checks. What's the essence of it?

While most AI-generated forgeries still lack the naturalness needed for convincing liveness sessions, organizations seeking maximum security should work exclusively with physical objects – no scans, no photos – just real documents and real people.

In the ID verification process, the solution must validate both the liveness and authenticity of the document and the individual presenting it.

This should also be supported by an AI verification model trained to detect even the most subtle video or image manipulations, which might be invisible to the human eye. It can also help detect other parameters that could flag abnormal user behavior. This involves checking the device used to access a service, its location, interaction history, image stability and other factors that can help verify the authenticity of the identity in question. It's like piecing together a puzzle to determine if everything adds up.

And one final tip – requesting that customers use their mobile phones during liveness sessions instead of a computer's webcam would be helpful. This is because it is generally much more difficult for fraudsters to swap images or videos when using a mobile phone's camera.

To wrap it up, AI is the ultimate sidekick for the good guys, ensuring the bad guys can’t sneak past those defenses. Still, AI models need guidance from us humans to stay on the right track. But when together, we are superb at spotting fraud.

https://www.entrepreneur.com/science-technology/deepfakes-are-on-the-rise-will-they-change-how/458415