Come explore with us! It should make it much harder to trick people with audio deepfakes Scammers can use AI to create deepfake mimics of people’s voices. But researchers are fighting back. They’ve found a way to trick the tricksters and protect others from impersonating your voice. Moor Studio/DigitalVision Vectors/Getty Images Plus By Kathryn Hulick 8 hours ago Imagine scrolling through TikTok and seeing famous YouTuber MrBeast pop up. He says he’s giving away brand-new iPhones. “Click the link below to claim yours now!” Do you click? Maybe. It sure looks and sounds like MrBeast. But it’s actually a deepfake — a phony clip created by artificial intelligence, or AI. Last October, this TikTok clip tricked some fans into sharing personal details. They also paid shipping fees for a phone that would never arrive. But a new tool — AntiFake — could help prevent such scams. Most deepfake defenses simply scan existing video or audio files to try to see if they’re real. AntiFake is different. It aims to protect recordings of our voices so that deepfake AI models have more trouble learning to mimic them in the first place. That could make it harder for AI to create voices for deepfake videos. It also could make it harder to create deepfake voices for phone scams. In some of those scams, crooks have used deepfake voices to call someone’s family members asking for money. In others, scammers have used the same technique to break into people’s voice-protected bank accounts. “We have seen that attackers use [AI tools] to conduct financial fraud or trick our family and friends,” says Zhiyuan Yu. “This is a real risk.” Yu is a PhD student in computer science at Washington University in St. Louis, Mo. He worked with the university’s Ning Zhang to build AntiFake. The computer scientists described their research at the 2023 ACM Conference on Computer and Communications Security. It was held in Copenhagen, Denmark, last November. AntiFake complements past work by other groups that guards images against deepfake copycats by AI. “How do we make sure society is using AI responsibly?” asks Zhang. “That’s the ultimate goal of our work.” Weekly updates to help you use Science News Explores in the learning environment Thank you for signing up! There was a problem signing you up. All it takes to create a deepfake voice is real audio or video of someone talking. Often, an AI model can learn to mimic someone’s voice based on just 30 seconds or so of speech. It does this by creating something called an embedding. This is basically a “series of numbers,” says Yu. The numbers are like an address to the speaker’s identity in a vast mathematical map of all voices. Voices that sound similar are located closer together in this map.