BIOMETRIC
UPDATE.COM

About Us | Subscribe

All Content ⌄   Search

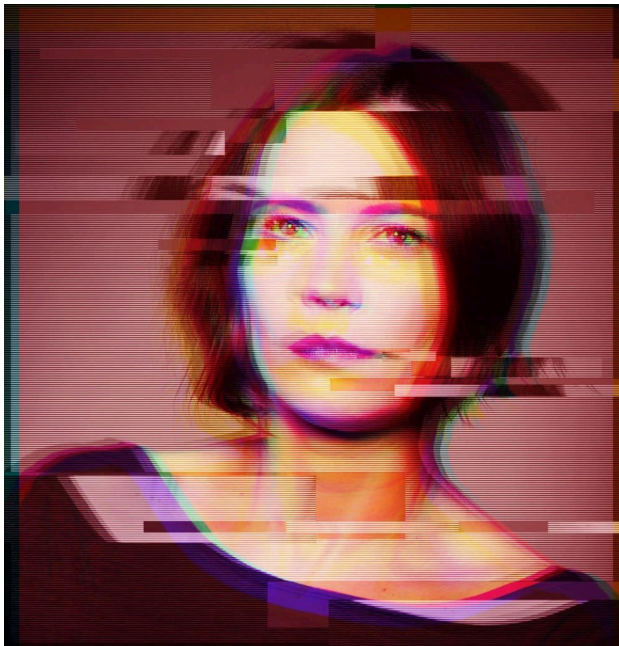| BIOMETRICS NEWS | DIGITAL ID FOR ALL | FEATURES & INTERVIEWS | INDUSTRY INSIGHTS | BRAND FOCUS | BIOMETRICS COMPANIES | EXPLAINING BIOMETRICS | WHITE PAPERS & WEBINARS | BIOMETRICS EVENTS |

Share

X/Tweet

Link

Comment

Only 0.1% of people can tell a deepfake, says iProov

Feb 12, 2025, 5:57 pm EST | Masha Borak

CATEGORIES   Biometrics News | Liveness Detection

Only a tiny fraction of people – 0.1 percent – can accurately distinguish between real and fake content such as images and video, according to new research on deepfakes conducted by iProov. Despite these abysmal results, around 60 percent of individuals said they were confident in their deepfake detection skills.

During its survey, the biometric identification company asked 2,000 UK and U.S. to look for deepfakes. The results showed that older generations are more vulnerable to deepfakes: One in five consumers stated that they were not even familiar with the concept. Young people, however, tended to be overly confident in their capability to spot fake content.

MOST VIEWED THIS WEEK

EU investigating Atos over buying EES software through Russian office

Trump, Musk, and their dangerous AI-driven government overhaul

Cameroon's new generation biometric ID card system goes live Feb 17

Biometrics connecting ID and payments through digital wallets, apps and passkeys

Mobile driver's licenses on the cusp of 'major paradigm shift'

Identity fraud for FEMA disaster relief raises questions on timeline for digital ID

NIMC's new Nigeria ID4D project partner to increase financial inclusion

Gesture-based age estimation tool BorderAge joins Australia age assurance trial

The results show that many organizations and consumers are vulnerable to identity fraud, according to Andrew Bud, founder and CEO of iProov. The company argues that organizations should adopt biometric-based solutions with liveness detection to verify whether someone is a real person.

"Even when people do suspect a deepfake, our research tells us that the vast majority of people take no action at all," says Bud. "Criminals are exploiting consumers' inability to distinguish real from fake imagery, putting our personal information and financial security at risk."

The survey participants were also 36 percent less likely to spot a synthetic video compared to a synthetic image, leading to the conclusion that deepfake videos are more challenging to identify compared to images.

UK companies facing surge of deepfake fraud

A report from fraud-prevention software maker Trustpair, on the other hand, shows how UK businesses are dealing with the surge of synthetic media fraud.

According to its data, 42 percent of companies have experienced at least two successful attacks with generative AI and deepfakes in the past year. The survey was based on interviews with 150 senior finance, treasury and accounts payable executives across the country.

Nearly three-quarters of the firms expect deepfake risks to grow in 2025 and have increased investment into fraud prevention technology. However, only 33 percent have invested in automated fraud prevention systems while many still rely on manual methods, such as callbacks and email-based validations.

Trustpair offers automated vendor account verifications to detect anomalies or suspicious transactions.

"The rise of AI-driven fraud demands a fundamental shift in how businesses approach payment security," says Tom Abbey, senior fraud consultant at Trustpair UK. "Companies cannot rely solely on human intervention to counter such sophisticated attacks. Automation is the only way to stay one step ahead of cybercriminals."

Reliance on social media could lead to greater vulnerability to deepfakes

New research from Nanyang Technology University (NTU) in Singapore seems to confirm iProov's thesis that

people are overconfident in their deepfake detection skills.

The scientists found that people who see the same deepfake video multiple times are more likely to believe it is true. This is because people are more likely to believe information is true if they hear it multiple times, regardless of its accuracy. The psychological phenomenon is called the "illusory truth effect."

The study involved more than 8,000 people from Singapore, China, Indonesia, Malaysia, the Philippines, Thailand, the U.S. and Vietnam. Participants were shown viral deepfake videos of media personality Kim Kardashian, Meta founder Mark Zuckerberg, Russian President Vladimir Putin and actor Tom Cruise.

Those participants who had seen a viral deepfake of the celebrity before the study were more likely to believe its contents once they had been exposed to it again. NTU researchers also found that people who get their news from social media for news instead of dedicated news sources, such as news websites, newspapers and TV, are more likely to accept false claims as true.

"Given that mere exposure to deepfakes could reinforce false beliefs, policymakers could consider psychological mechanisms (such as the illusory truth effect) when developing educational campaigns focused on debunking deepfakes," says Saifuddin Ahmed, assistant professor at NTU.

The study was published in the Journal of Broadcasting & Electronic Media.

Article Topics

biometrics | deepfake detection | deepfakes | fraud prevention | iProov

Latest Biometrics News

Age assurance in shops reduces lineups, eases staff burdens and improves security

Feb 12, 2025, 7:05 pm EST

Age assurance technologies are increasingly being deployed for point-of-sale use cases, and proving effective at curtailing the sale of restricted...

Amazon firm: fired worker deserved it. Less so on its cop FR ban

Feb 12, 2025, 6:23 pm EST

The wrongful-firing lawsuit filed against Amazon Web Services in the UK has gained a new life. An October dismissal of...

Ukraine tests compatibility with EUDI Wallet

Feb 12, 2025, 5:27 pm EST

Ukraine has successfully tested its compatibility with the European Union Digital Identity (EUDI) Wallet, allowing its citizens to use digital...

North Carolina, Arkansas work toward mDL launches

Feb 12, 2025, 5:05 pm EST

BIOMETRICS EVENTS

LivDet 2025: Fingerprint Liveness Detection Competition
Online: Feb 1 - Apr 20, 2025

Enterprise AI Turkey Summit 2025
Istanbul, Turkey: Feb 18 - Feb 19, 2025

18th Edition Connected Banking Summit – Innovation & Excellence Awards – West Africa 2025
Accra, Ghana: Feb 19, 2025

EAB Lunch Talk – Biometric-bound credentials: Enhancing security and flexibility in digital identity
Microsoft Teams: Feb 19, 2025

Identity & Payments Summit
San Diego, CA: Feb 24 - Feb 26, 2025

More Biometrics Events

The strategic plan for North Carolina's implementation of mobile driver's licenses (mDLs) is contained in a study published in revised...

Nametag secure onboarding and ID verification bars entry to IT plants

Feb 12, 2025, 5:01 pm EST

The United States' latest tool in clamping down on North Korean espionage? Look no further than Nametag's integrated identity verification...

Appeals court orders NYPD facial recognition contracts made public

Feb 12, 2025, 4:49 pm EST

An appeals court in New York has ruled that the New York Police Department (NYPD) must disclose all documents relating...

Comments

Leave a Reply

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Biometrics News   Brand Focus   Research   White Papers   Companies   Solutions   Request a quote

Events   Biometrics in developing nations

About Us   Advertise   Media Kit   Free Listings   Submit a Press Release   Contact Us   Jobs   Privacy Policy