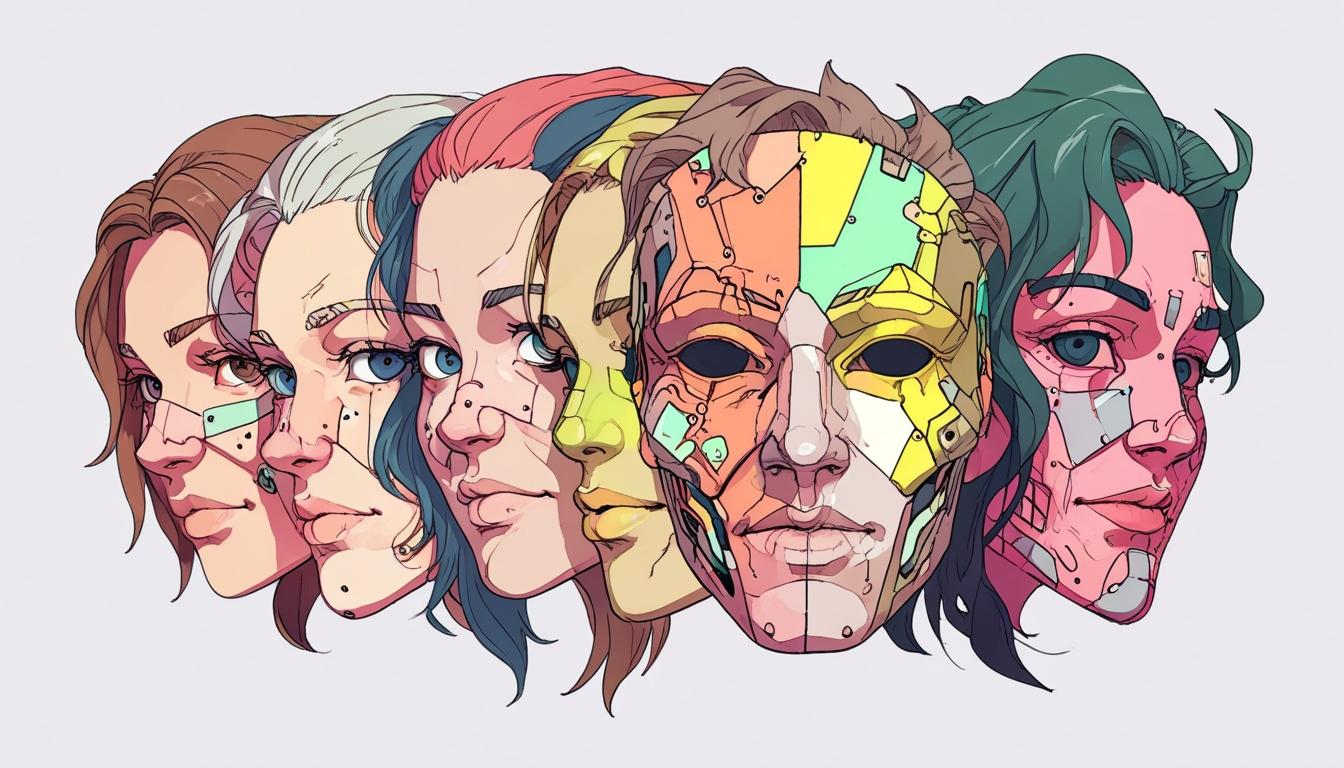
# Oxford study reveals surge in deepfake tools disproportionately targeting women



# The Alarming Rise of Deepfake Technology: An Oxford Study Sheds Light on the Growing Threat

Researchers at the Oxford Internet Institute (OII) have revealed a disquieting trend in the proliferation of deepfake technology, identifying nearly 35,000 AI tools available for public download that can generate deepfake images of identifiable individuals. This alarming increase was highlighted in their detailed study, titled 'Deepfakes on Demand,' which found that these deepfake generators have been downloaded almost 15 million times since late 2022. The study underscores a troubling reality: the vast majority of these impersonations (96%) target identifiable women, including both well-known celebrities and ordinary social media users.

Lead author Will Hawkins, a doctoral student at the OII, emphasised the urgent need for enhanced technical safeguards and more robust regulatory measures to combat the creation and distribution of harmful AI models. Hawkins stated, “There is an urgent need for more robust technical safeguards, clearer and more proactively enforced platform policies, and new regulatory approaches to address the creation and distribution of these harmful AI models.” Given the low cost of producing these deepfakes, the researchers warn that even more egregious content—such as child sexual abuse material—could be on the rise, potentially lurking beyond public platforms.

The troubling implications of this study connect to a wider narrative involving the misuse of deepfake technology. Prominent figures like Martin Lewis, the founder of MoneySavingExpert.com, have become unwitting victims of deepfake scams. Lewis recently took to social media after discovering a fake video featuring him promoting a fraudulent investment scheme, an experience he characterised as “weird and pretty frightening.” He echoed calls for regulatory action, highlighting the urgent need for measures to protect consumers from these increasingly sophisticated scams.

Indeed, deepfake scams have become a growing concern. The Financial Times reports on how generative AI enables scammers to create convincing fake videos, often impersonating public figures to promote fraudulent investment schemes on platforms like Instagram and WhatsApp. Experts have urged users to remain vigilant, noting that many social media users are unaware of the capabilities of AI, making them more susceptible to these deceptive practices. Social media companies, while claiming to combat such content through AI moderation, have faced criticism for their inadequate responses.

Recent statistics bolster the urgency for regulatory action. Reports from the Revenge Porn Helpline indicate a dramatic increase in intimate image abuse, with instances rising by 20.9% in 2024, culminating in a total of 22,275 reports—the highest figure in the helpline's history. The UK government has taken steps to address this issue, making the sharing of sexually explicit deepfake images a criminal offence under the Online Safety Act as of April 2023. Additional proposals aim to criminalise the creation of such content as part of the ongoing Crime and Policing Bill.

Efforts are being made at various levels to hold technology companies accountable. Rafał Brzoska, the head of InPost, is seeking to enlist around 150 notable Polish figures to sue Meta for the proliferation of deepfake scams using AI-generated impersonations on its platforms. Brzoska's initiative reflects a broader push for accountability in the tech industry, a sentiment echoed by Lewis, who warned against the “wild west” nature of current tech regulations, calling for immediate legislative action to protect vulnerable individuals from scams.

As the study from the Oxford Internet Institute suggests, society is witnessing only the tip of the iceberg when it comes to deepfake technology. The potential for more significant and harmful content looms large, underscoring the imperative for a unified and effective response. The technology’s rapid advancement poses a fundamental question: how can we balance the benefits of AI innovation with the pressing need for safeguarding users against its darker applications? This dialogue is becoming ever more critical as deepfakes increasingly infiltrate our digital lives.

## Reference Map:

* Paragraph 1 – [[1]](https://www.oxfordmail.co.uk/news/25144023.oxford-university-uncovers-dramatic-rise-deepfakes/?ref=rss)
* Paragraph 2 – [[1]](https://www.oxfordmail.co.uk/news/25144023.oxford-university-uncovers-dramatic-rise-deepfakes/?ref=rss), [[4]](https://www.bbc.com/news/uk-66130785)
* Paragraph 3 – [[2]](https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123), [[3]](https://www.ft.com/content/f390bf57-d3bd-4462-a722-cd1b755589a3)
* Paragraph 4 – [[5]](https://www.finextra.com/newsarticle/42612/martin-lewis-calls-for-regulation-after-featuring-in-deepfake-ai-scam), [[6]](https://www.univ.ox.ac.uk/news/deepfake-technology/)
* Paragraph 5 – [[4]](https://www.bbc.com/news/uk-66130785), [[3]](https://www.ft.com/content/f390bf57-d3bd-4462-a722-cd1b755589a3)
* Paragraph 6 – [[1]](https://www.oxfordmail.co.uk/news/25144023.oxford-university-uncovers-dramatic-rise-deepfakes/?ref=rss), [[5]](https://www.finextra.com/newsarticle/42612/martin-lewis-calls-for-regulation-after-featuring-in-deepfake-ai-scam)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.oxfordmail.co.uk/news/25144023.oxford-university-uncovers-dramatic-rise-deepfakes/?ref=rss> - Please view link - unable to able to access data
2. <https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123> - The Financial Times reports on the rapid growth of deepfake scams, highlighting how generative AI technology enables scammers to create convincing fake videos impersonating public figures. These deepfakes are used to promote fraudulent investment schemes on platforms like Instagram and WhatsApp. Experts warn that many social media users are unaware of AI's capabilities, making them more susceptible to these scams. Social media companies, including Meta, claim to combat this content using facial recognition and AI tools but have faced criticism for inadequate content moderation and slow response. The UK's new Online Safety Act requires quicker removal of illegal material. To avoid falling victim, users are advised to critically assess video authenticity by examining mouth movements, skin texture, eye behavior, and voice tone. It's crucial to report impersonations and alert others to prevent further spread of scams.
3. <https://www.ft.com/content/f390bf57-d3bd-4462-a722-cd1b755589a3> - Rafał Brzoska, a Polish billionaire and head of InPost, is seeking support from prominent Polish figures to sue Meta over the proliferation of 'deepfake' scams using AI-generated impersonations on its platforms. Brzoska aims to include around 150 notable Polish individuals, including former presidents and prime ministers, in the lawsuit. He previously secured an injunction to halt the spread of fake news and images of himself and his wife on Meta's platforms. This action follows similar pressures on Meta, such as a lawsuit permitted by a U.S. judge for Australian billionaire Andrew Forrest. Meta, emphasizing its policy against deceptive ads, has indicated continued efforts to counter scams. Brzoska hopes the EU's strong regulations on data protection will support his case and set a precedent for other victims globally.
4. <https://www.bbc.com/news/uk-66130785> - Martin Lewis, the founder of MoneySavingExpert.com, expressed his shock and concern after encountering a deepfake scam video featuring his likeness. The video, which appeared on Facebook, used AI technology to create a realistic imitation of Lewis endorsing a fraudulent investment scheme. Lewis described the experience as 'weird and pretty frightening' and emphasized the need for regulation to prevent such scams. He highlighted that many people could be tricked into losing money without proper industry oversight. The incident underscores the growing prevalence of deepfake technology in online scams and the challenges in detecting and preventing them.
5. <https://www.finextra.com/newsarticle/42612/martin-lewis-calls-for-regulation-after-featuring-in-deepfake-ai-scam> - Consumer finance specialist Martin Lewis has spoken out after a deepfake scam video featuring his likeness was circulated on Facebook. The ad aims to trick people into investing in a fake project backed by Elon Musk, using a computer-generated version of Lewis to promote consumers to participate. Lewis called the ad 'weird and pretty frightening', and urged consumers to stay vigilant before transferring funds to unknown sources. He emphasized that regulation of the tech industry amounts to a 'wild west' situation and called on the government to press ahead with legislation. Lewis added: 'We are scared of big tech in this country and we need to start regulating them properly. Vulnerable people are being scammed and nothing is being done about it.'
6. <https://www.univ.ox.ac.uk/news/deepfake-technology/> - Andrew Lewis, a DPhil Politics student at the University of Oxford, co-authored a study on deepfake technology and content moderation. The research, funded by the Royal Society, found that people are not good at discerning quality deepfakes from genuine videos. Even when warned that at least one of the five videos they view has been altered, 78% of participants still cannot spot the deepfake. The study highlights the inadequacy of human discernment in detecting deepfakes and raises concerns about the effectiveness of warning labels. The findings suggest that successful content warnings on deepfakes will rely on trust in moderators' judgments, which could be perceived as politically motivated or biased.
7. <https://en.wikipedia.org/wiki/Deepfake> - Deepfake technology involves the use of artificial intelligence to create convincing images, audio, and videos that depict individuals saying or doing things they did not actually do. This technology has been increasingly used in fraudulent activities, including scams and misinformation campaigns. Deepfakes have been used to impersonate celebrities and politicians, leading to significant financial losses and reputational damage. The Better Business Bureau reports that deepfake scams are becoming more prevalent, with an estimated $12 billion in fraud losses globally. The technology was developed by a London company called Synthesia, which markets it as a cheap alternative to live actors for training and HR videos.