

IN THE NEWS

What you need to know about deepfakes

Taylor Swift is the most recent celeb to fall prey to sexually explicit AI imagery – and it could happen to anyone with a social media account. So how to stay protected? Read on

In January, pornographic deepfakes of one of the world's most powerful women – Taylor Swift – were viewed 47 million times on X (formerly Twitter), before being taken down. In addition to being intensely shocking, the incident highlighted the rise of one of social media's biggest ethical dilemmas, and it's not just affecting celebs.

So, what's a deepfake? It's an image created with AI, using an existing photo or video of someone that's manipulated to make them look and sound like another person. In short, deepfakes make the subject appear to do or say something they didn't.

A report by Home Security Heroes found online deepfake videos increased 550 per cent between 2019 and 2023. Ninety-eight per cent of content is sexually explicit and 99 per cent of subjects are women – in most cases, without their consent.

Deepfakes can be made in minutes using apps or YouTube tutorials, and they're being used to scam, spread disinformation or defame victims. While it's something A-listers have long had to contend with, it's increasingly filtering into the wider world.

"I know of a woman who shared content on LinkedIn about celebrating an achievement in the workplace," recalls Yasmin London, director of digital resilience at ySafe. "Someone captured her image, created a pornographic deepfake and circulated it online to defame and discredit her."

That said, not all deepfakes are nefarious. Popular TikTok account @DeepTomCruise posts hilarious Tom Cruise videos. Robin Wright and Tom Hanks have been 'de-aged' to play their characters' younger selves in an upcoming film using face-replacement tech. And Spotify is trialling AI that translates podcasts into other languages – all in the host's own voice.

But the most important questions are: how do you protect your happy snaps and home vids, and what can victims do?

"The only way to safeguard yourself is to have no digital footprint," says branding coach, Kate Heussler. "But that's not realistic." Last year, Heussler discovered that her photos and identity had been misappropriated in an online romance scam. A fraudster posing as Heussler lured a US-based man into an online relationship and asked him for money. While initially



“
The only safeguard is to have no digital footprint. But that's not realistic

– KATE HEUSSLER

horrified, Heussler says that, at 40, she had the emotional maturity to cope. "If it happened to me as a teenager, I'd be so humiliated. I'm concerned about this happening to young girls."

Sadly, the law is lagging when it comes to this issue. "Australia currently has no targeted legislation that specifically addresses the misuse of deepfake content," says Prabha Nandagopal, a human rights lawyer and the founder of Elevate Consulting Partners. "To take action against someone who has created or shared deepfakes, whether under civil or criminal laws, the victim needs to sue or the police need to charge someone. And unfortunately, people who create or share deepfakes can be incredibly difficult to find."

It's still important to report illegal imagery, even if you're not the target. Contact the police, the eSafety Commissioner (esafety.gov.au) or, if children are involved, the Australian Centre to Counter Child Exploitation (accce.gov.au). You can also request the platform or website remove the content. "Take the time to report it," says London. "Because every set of eyes that sees it is just re-victimising the person in the picture." London also advises switching personal social media accounts to private and rethinking posting images of your kids.

Keep online videos short, suggests James Cook University lecturer, Dr Dan Miller. "Photos in which you aren't facing the camera make it more difficult to create a realistic deepfake."

Finally, the obvious: don't believe everything you see online.

+ **CLICK** WANT MORE? READ OUR EXTENDED STORY NOW AT **BODYANDSOUL.COM.AU**