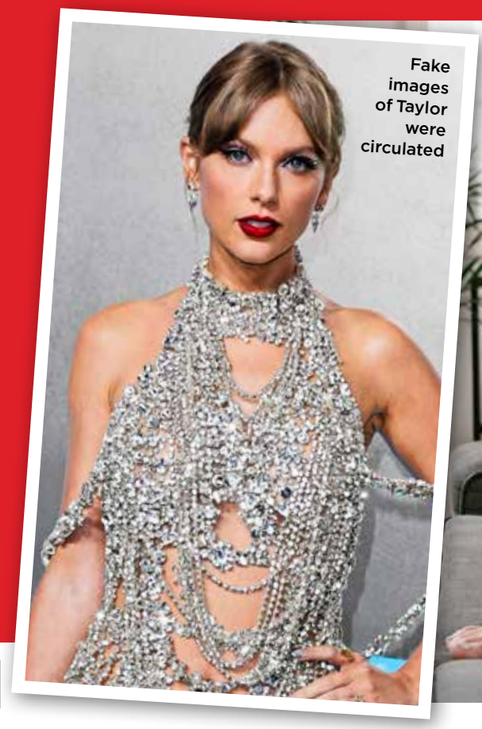
HOW YOU CAN PROTECT YOU RSELF FROM BECOMING A VICTIM OF DEEPFAKE PORN

Taylor Swift became the latest celebrity to become the target of a deepfake porn site – where AI-generated sexually explicit images of her began circulating – last month, particularly gaining traction on social media sites including X, formerly known as Twitter. Dozens of graphic images were uploaded to Celeb Jihad, which show 'Taylor' in a series of sexual acts while dressed in Kansas City Chief memorabilia and in the stadium. One image was seen 47 million times in the 17 hours it was live, before it was removed.

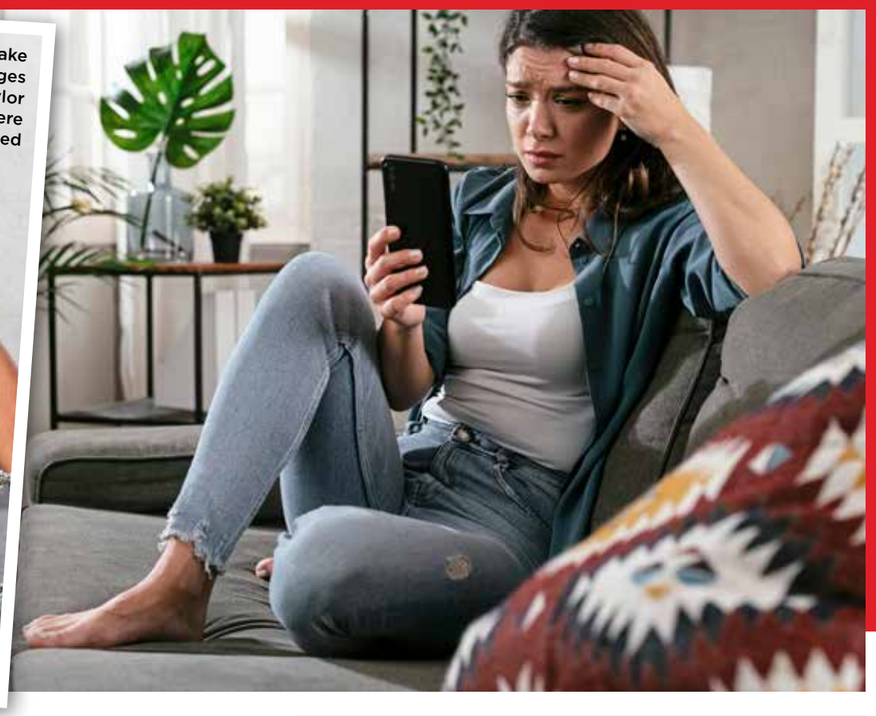
She's not the first public figure to have been targeted using deepfakes – a term used to describe any digitally-manipulated image or video that can look convincingly real. Images and videos can be generated from scratch by feeding AI tools with prompts of what to display. Alternatively, the face of someone in a video or image can be swapped out with someone else's, such as a famous person.

This latest attack has renewed calls to strengthen legislation around AI, particularly when it is misused for sexual harassment. A source close to Taylor said, "Whether or not legal action will be taken is being decided, but there is one thing that is clear: these fake AI-generated images are abusive, offensive, exploitative and done without Taylor's consent and/or knowledge... The door needs to be shut on this. Legislation needs to be passed to prevent this and laws must be enacted."

And as AI grows, deepfake porn is becoming an increasing problem in the UK too – one site that virtually strips women received 38 million hits in the first eight months of 2021. Closer speaks to mum Sophie Parrish, who has experienced the torture of fake AI images first hand.



Fake images of Taylor were circulated



MUM-OF-TWO:

'This could happen to anybody'

Sophie was featured in fake images online

Sophie Parrish, 31, from Merseyside, lives with her husband Mark, 36, and their two children. She tells *Closer* why she hopes her petition will help change UK laws surrounding digitally-created revenge porn to give victims the justice they deserve.

She says, "In September 2022, I got a Facebook message request from someone I didn't know. Opening it, the message read, 'I've seen photos of you. I know where you live'. Underneath the message, attached, were sexually explicit photos and videos. I was horrified and disgusted.

"When my husband Mark got home, he was livid and said we needed to call the police. They were helpful when taking my statement, but I still felt incredibly anxious. I confided in my friends and family, who were as stunned as I was.

"A few weeks later, I met my cousin at the gym. She looked really upset. 'I've seen something really dark', she said. 'There are images of you on this website where you're naked, but I don't think it's you. It's definitely your face, but it's not your body'. I thought she was joking and couldn't understand what she was saying. Then she handed me her phone and I scrolled in horror. My face had been edited onto naked pictures of other women. They were graphic and showed women with their legs spread. There were also pictures of men who'd pleasured themselves over the photos. I didn't know how to process it, and ran to the toilet to be sick.

'INNOCENT PEOPLE SHOULD NOT BE USED FOR THIS KIND OF CONTENT'

INFURIATED

"I drove to my parents' house and showed them the photos. I knew they wouldn't have believed me or understood unless I showed them. I then rang Mark, who was furious and said I had to call the police. As they took my statement, I felt dirty, violated, ashamed and angry.

"I'd heard of deepfake porn but had never really taken notice, never in a million years believing it could be something that would happen to me. I contacted the owner of the website where the photos came from, but they said because the pictures were fantasy and didn't technically show real people, they did not have any rights to remove them. This infuriated me beyond words.

"On 30 January 2023, police told me a man was arrested on suspicion of disclosing or threatening to disclose private sexual photographs and films with intent to cause distress but, after an investigation, no action was taken. There were no laws in place for deepfakes at the time, so it made my case extremely difficult. He just walked away with no punishment.

"Now I just hope my kids don't ever see those pictures – but they know something's happened, as I haven't been myself.

"After the investigation was dropped, I launched a petition as I don't believe this should happen to other women and for people to get away with it. My dignity and my privacy were completely compromised. I want it to be illegal to create and share explicit images without consent, and my petition now has more than 1,200 signatures.

"The laws have changed since what happened to me. The Online Safety Act now makes it a criminal offence to share, or threaten to share, a manufactured or deepfake intimate image or video of another person without his or her consent, but it is not intended to criminalise the creation of such deepfake content, which I think is wrong.

HORRENDOUS

"I no longer feel as ashamed as I did, thanks to counselling, but I'm not the same person I was. Innocent people should not be used for this kind of content, especially when it's non-consensual. I want to urge women to be careful what they post online. What the perpetrator has done is horrendous, but my biggest piece of advice now is, speak out if it's happened to you – don't stay quiet."

● *Sign the petition at change.org/p/deepfake-porn-make-it-illegal-to-create-and-and-share-explicit-images-without-consent*

TIPS TO KEEP YOURSELF SAFE

- Limit the amount of data available about yourself, especially high-quality photos and videos that could be used to create a deepfake. You can enable strong privacy settings on social media to restrict who can see your photos, videos and other data.
- When sharing images or videos online, consider using a digital watermark on them. This can discourage deepfake creators from using your content since it makes their efforts more traceable.
- Learn about deepfakes and AI. Staying abreast of the latest developments can help you stay vigilant. You don't need to become an expert, but following the news about these technologies is important.
- These days, you really should double your security by implementing multi-factor authentication for all of your accounts. This is when you need an extra step to log into an account, such as a facial scan, entering a code texted to your phone, or using a standalone app on your device. This extra layer of security helps prevent unauthorised access to your accounts.
- Use long, strong passwords. Passwords should be at least 16 characters long, and contain a random mix of upper case letters, lower case letters, numbers and special characters.
- Report deepfake content. If you come across content that involves you or someone you know, report it to the platform hosting the content. This can help in having it removed or investigated, limiting its potential reach. You should also report it to the police.
- ***For more information, go to staysafeonline.org***

PHOTOS: SHUTTERSTOCK, PA REAL LIFE