



CYBERCRIME: THE RISING SCALE OF DECEIT



A brief history of deception



1980s MALWARE

A 15-year-old prankster deploys the first large-scale computer virus outbreak in history, affecting the Apple II OS.



1990s HACKING GOES MAINSTREAM

As hackers adapt to the emergence of the World Wide Web.



YEAR 2000 DDOS SURGE

The cost of cybercrime skyrockets at the turn of the century when the infamous MafiaBoy DDoS attack results in over USD 1 billion in damages, impacting the likes of Amazon, eBay and Yahoo¹.



LATE 2010s THE DAWN OF DEEPAKES

Artificial Intelligence (AI) enables the mass creation of 'deepfakes': video and audio that closely resemble real people, which can be manipulated for misleading political or criminal intent.



MID 2000s RISE OF RANSOMWARE

Ransomware increasingly wreaks havoc around the world with hackers targeting individuals as well as businesses.



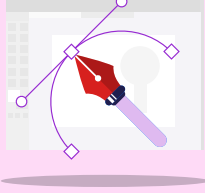
EARLY 2000s ID THEFT

With a growing volume of personal data being stored globally across servers and online, digital identities start to come under attack at scale.

The scale of deception

PHOTOSHOPPING

Easy, convincing and widely available way of manipulating still images



SHALLOW FAKES

Simple manipulation of images and videos



AUDIO DEEPAKES

Copying someone's voice



LIP SYNC

Creating video of someone speaking by synthesising publicly-available audio and video of them



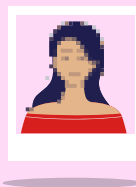
BIOMETRIC FAKES

An emergent threat to corporate virtual identity verification



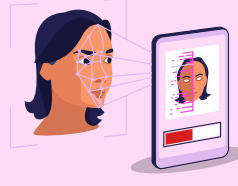
COMPUTER GENERATED IMAGERY

CGI – extremely expensive, theatrical productions, entertainment-only



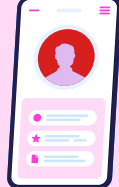
FACE SWAP / DE-CLOTHED

Almost exclusively non-consensual images of women



PUPPETRY

Mapping a target's face onto an actor's, having them say or do things they didn't



FAKE PEOPLE

Social media sites such as LinkedIn contain many fake companies with fake employees with synthesised imagery

Double-takes

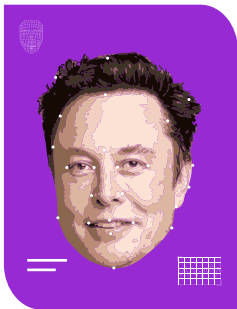
Well-known identities who have been famously 'deepfaked' include:



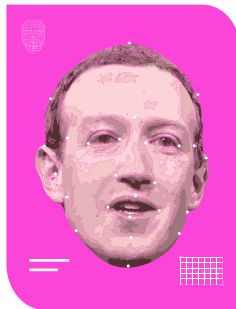
Barack Obama



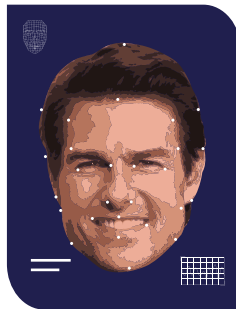
Boris Johnson



Elon Musk



Mark Zuckerberg



Tom Cruise

Identity crisis



Reddit bans 'r/deepfakes' community of **90,000** users².



LinkedIn removed **21 MILLION** fake profiles³.



There were more than **60,000** synthetic videos (typically referred to as 'deepfakes') posted online⁴.



The CEO of a UK energy firm was tricked into sending **USD 240,000** to a supplier after receiving a deepfake audio phone call, supposedly from the CEO of his company's parent firm⁵.



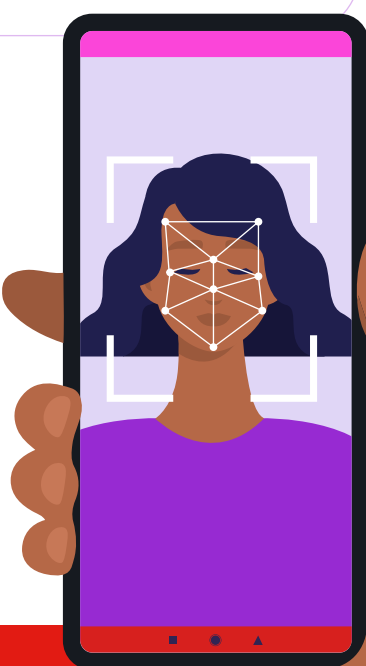
Sensity reports the number of deepfake videos online doubled every six months in the past three years⁶. Last count: **85,047**



Facebook announced it will remove videos modified by artificial intelligence, known as deepfakes, from its platform⁷.



Deepfake detection company Sensity uncovered more than **100,000** images on Telegram, a messaging platform similar to WhatsApp, where a Russia-centric bot was maliciously manipulating images of women⁸.



How to spot visual deepfakery



Blurred/meaningless background.



Textures are inconsistent (hair and clothing fibres are harder to synthesise than facial features).



They can be asymmetrical (for example, earrings won't match).



Good looks – synthesised images do not accommodate flaws or idiosyncracies.



"It looks scary, but remember, there is far more capability to defend against these deceptions than is commonly talked about."

SIMON BROWN

Head of Cybersecurity Strategy and Capability at Westpac

Sources

- <https://www.britannica.com/technology/denial-of-service-attack>
- <https://www.theguardian.com/technology/2018/feb/08/reddit-bans-deepfakes-face-swap-porn-community>
- <https://blog.linkedin.com/2019/august/20/an-update-on-how-were-fighting-fake-accounts>
- <https://westpac.westpac.com.au/Article/46702>
- <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=3339aeb62241>
- <https://sensity.ai/reports/>
- <https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/>

