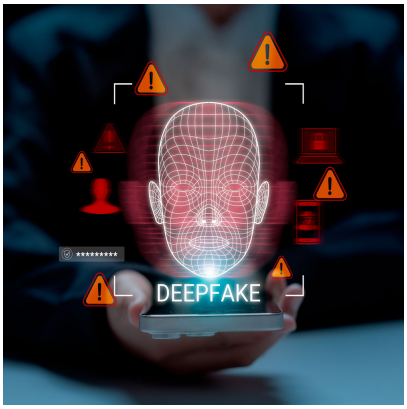

That’s a fake!

Description

Deepfake technology poses serious threats to both our personal security and organisational integrity, making detection skills essential to protect us against sophisticated digital deception.

As artificial intelligence (AI) becomes more sophisticated, deepfake technology has emerged as a significant concern because these hyper-realistic – but fabricated – videos and audio recordings can be used for financial fraud, reputation damage, and disinformation campaigns.

AfroCentric Technologies recently hosted a webinar on AI and how to spot a deepfake.

Understanding deepfake technology

Deepfakes use advanced AI algorithms to create convincing fake videos, audio recordings or images of real people. These sophisticated forgeries can make it appear that someone said or did something they never actually did. Cybercriminals exploit this technology for various malicious purposes, including financial scams, political manipulation, and personal harassment.

Keep your eyes and ears open

Detecting deepfakes requires careful observation of subtle inconsistencies. Visual clues include unnatural blinking patterns, inconsistent lighting across facial features, poor lip-syncing and overly smooth or distorted facial characteristics. Audio deepfakes may lack emotional nuance or natural speech patterns, even when the voice sounds convincing.

Equally important is the context – does the scenario depicted align with reality or expected behaviour?

Always scrutinise the credibility of platforms sharing such content and research the original source of suspicious material.

Verify independently

Independent verification forms the backbone of detecting a deepfake. Compare dubious content with legitimate sources such as verified social media accounts or official websites. Use multiple communication channels to confirm authenticity, particularly when dealing with urgent requests involving financial transactions or sensitive information.

Fact-checking platforms such as Africa Check and AFP Fact Check provide valuable resources for verifying suspicious claims before sharing them. These tools help to combat the spread of misinformation and protect communities from deepfake deception.

How to spot a deepfake

1. Examine closely: Look for visual inconsistencies such as uneven lighting, unnatural blinking or poor lip-syncing in suspicious videos.
2. Question urgency: Be wary of content that creates artificial time pressure or fear-based decision-making scenarios.
3. Verify independently: Use official channels and trusted sources to confirm information rather than relying solely on suspicious content.
4. Trust your instincts: If something feels “off” about a video or audio recording, investigate further before acting.
5. Use multiple channels: Confirm requests through different communication methods, especially for financial or sensitive matters.
6. Establish code systems: Create family or organisational authentication methods to verify critical communications.
7. Stay informed: Keep up with emerging deepfake trends and detection techniques through reputable cybersecurity resources.

Protecting yourself and our business against deepfakes requires vigilance, scepticism and systematic verification practices. By developing these detection skills and maintaining an awareness of evolving threats, we can better defend ourselves against sophisticated digital deception. Remember that in the age of AI-generated content, healthy scepticism is your best defence!

Category

1. Our Knowledge Centre