Incident 983: Scammers Reportedly Used AI Voice Clone and YouTube Footage to Impersonate WPP CEO in Unsuccessful Scam Attempt

𝕏 in ✉ f ⬅ 🔀 ➡

Description: Scammers reportedly attempted to impersonate WPP CEO Mark Read using AI-generated voice cloning and YouTube footage in a Microsoft Teams scam. They allegedly created a fake WhatsApp account with Read's image and used deepfake audio to deceive an agency leader into setting up a new business. The scheme, which was unsuccessful, aimed to solicit money and personal data.

Tools

✉ Notify Me of Updates | + New Report | + New Response | 🔍 Discover | 66 Citation Info | ↺ View History

Entities

View all entities

Alleged: Unknown deepfake technology developer and Unknown voice cloning technology developed an AI system deployed by scammers , Fraudsters and Scammers impersonating Mark Read , which harmed Mark Read , WPP , WPP employees and General public .

Alleged implicated AI systems: Unknown voice cloning technology , Unknown deepfake app , YouTube , Microsoft Teams and WhatsApp

Incident Stats

Incident ID	983
Report Count	15
Incident Date	2024-05-10
Editors	Daniel Atherton

Incident Reports

Reports Timeline

Timeline

Jul 2024
- **+11** CEO of world's biggest ad firm targeted by deepfake scam
- WPP CEO Mark Read targeted by deepfake AI scam

October
- Deepfake scams escalate, hitting more than half of businesses

2025

April

July
- **+1** Deepfak...

CEO of world's biggest ad firm targeted by deepfake scam
theguardian.com

CEO of world's biggest ad firm targeted by deepfake scam

theguardian.com · 2024 ⌄

The head of the world's biggest advertising group was the target of an elaborate deepfake scam that involved an artificial intelligence voice clone. The CEO of WPP, Mark Read, detailed the attempted fraud in a recent email to leadership, wa...

Read More ↓
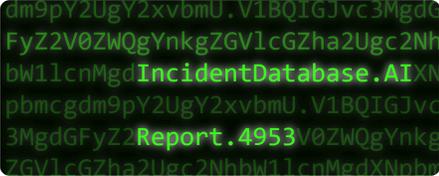
WPP boss targeted by deepfake scammers using voice clone

ft.com · 2024 ⌄

Mark Read, chief executive of WPP, has been the target of a deepfake scam in which criminals used a voice clone and public YouTube footage to set up a video meeting with his executives.

In an email to colleagues seen by the Financial Times,...

Read More ↓

WPP CEO Addresses Deepfake Scam Attempt

designrush.com · 2024 ⌄

WPP CEO Mark Read recently fell victim to a deepfake scam, with perpetrators attempting to defraud the advertising executive using sophisticated tactics involving AI-generated voice cloning and manipulated video footage.

In an email to comp...

Read More ↓

CEO of world's biggest ad agency falls victim to elaborate deepfake scam

nypost.com · 2024 ⌄

The CEO of WPP fell victim to an elaborate deepfake scam that involved voice-cloning the boss to solicit money and personal details from the company's workforce.

Mark Read, the CEO of WPP, a London-based communications and advertising compa...

Read More ↓

Boss of world's biggest ad firm impersonated by AI in elaborate deepfake scam

telegraph.co.uk · 2024 ⌄

The boss of one of the world's largest advertising companies was impersonated by artificial intelligence (AI) in an elaborate deepfake scam.

Fraudsters mimicked Mark Read, chief executive of WPP, in a recent video meeting in an attempt to s...

Read More ↓
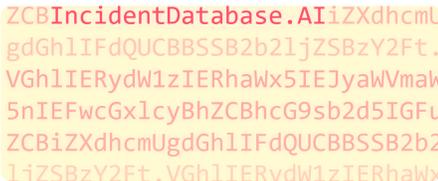
The Drum's Daily Briefing: Apple's ad apology and beware the WPP AI voice scam

thedrum.com · 2024 ⌄

Apple admits fault in iPad Pro campaign

Apple has issued an apology for its latest iPad Pro advertisement, which has been condemned for being "out of touch" with its creative community.

As we reported yesterday, few ads in recent memory hav...

Read More ↓

WPP CEO Mark Read targeted by deepfake attack

adgully.com · 2024 ⌄

WPP CEO Mark Read came under a phishing attack utilizing a sophisticated deepfake scam. Read's email to leadership detailed the incident, raising awareness about the growing threat of AI-powered scams exploiting virtual meetings and deepfak...

Read More ↓

WPP chief exec Mark Read targeted by deepfake scammers

mmm-online.com · 2024 ⌄

WPP chief executive Mark Read was the target of a deepfake scam involving an artificial intelligence voice clone.

Fraudsters set up a WhatsApp account with an image of Read and then used it to set up a Microsoft Teams meeting with another s...

Read More ↓

AI voice, fake WhatsApp account: How scammers targeted CEO of world's biggest ad firm using deepfake

timesofindia.indiatimes.com · 2024 ⌄

Mark Read, the CEO of WPP – the world's largest advertising company as of 2023 – has reportedly been targeted by scammers. A report says that fraudsters used a deepfake technique to set up a call but were unable to successfully execute the ...

Read More ↓

WPP CEO Impersonated in Deepfake Scheme to Steal Execs Money

entrepreneur.com · 2024 ⌄

As deepfakes become more prevalent, phishing attacks on companies have become more complex and harder to identify.

Last week, at the largest advertising agency in the world, London-based communications and advertising firm WPP, hackers atte...

Read More ↓

WPP CEO Mark Read targeted by deep fake AI scam

bizcommunity.com · 2024 ⌄

The scam was unsuccessful.

In a statement quoted by *The Guardian* a WPP spokesperson confirmed the phishing attempt bore no fruit. "Thanks to the vigilance of our people, including the executive concerned, the incident was prevented."

Report...

Read More ↓

WPP CEO Mark Read targeted by deepfake AI scam

marketing-interactive.com · 2024 ⌄

Mark Read (pictured), the chief executive officer of advertising agency WPP, has been the target of a deepfake scam that involved an artificial intelligence (AI) voice clone.

The scammers reportedly created a WhatsApp account using a publi...

Read More ↓

Deepfake scams escalate, hitting more than half of businesses

cybersecuritydive.com · 2024

- Just over half of businesses in the U.S. and U.K. have been targets of a financial scam powered by "deepfake" technology, with 43% falling victim to such attacks, according to a survey by finance software provider Medius.
- Of the 1,533 U.S....

Read More ↓
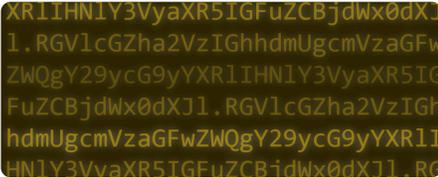
Deepfakes have reshaped corporate security and culture

scworld.com · 2025

COMMENTARY: In recent years, corporate Deepfake incidents have surged, with 53% of businesses reporting encounters. Initially perceived as mere digital entertainment on platforms like X and Instagram, Deepfakes have evolved into a formidabl...

Read More ↓

Why detecting dangerous AI is key to keeping trust alive in the deepfake era

weforum.org · 2025

The finance worker in Hong Kong thought nothing unusual about the video call. Their UK-based chief financial officer needed urgent approval for a confidential acquisition, and several familiar colleagues joined to discuss details.

After tho...

Read More ↓

Variants

A "variant" is an AI incident similar to a known case—it has the same causes, harms, and AI system. Instead of listing it separately, we group it under the first reported incident. Unlike other incidents, variants do not need to have been reported outside the AIID. Learn more from the research paper.

Seen something similar? ＋ Submit a Variant

Similar Incidents

By textual similarity ❓

Did **our** AI mess up? Flag 🚩 the unrelated incidents

Hackers Break Apple Face ID

Sep 2017 · 24 reports 🏳

Deepfake Obama Introduction of Deepfakes

Jul 2017 · 29 reports

Female Applicants Down-Ranked by Amazon Recruiting Tool

Aug 2016 · 33 reports

← Previous Incident

Next Incident →

Research

Defining an "AI Incident"
Defining an "AI Incident Response"
Database Roadmap
Related Work
Download Complete Database

Incidents

All Incidents in List Form
Flagged Incidents
Submission Queue
Classifications View
Taxonomies

Project and Community

About
Contact and Follow
Apps and Summaries
Editor's Guide

2024 - AI Incident Database

Terms of use
Privacy Policy

a9df9cf