



## Technology

🕒 This article is more than 1 year old

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

**Exclusive:** fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet

**Nick Robins-Early**

Fri 10 May 2024 03.01 EDT

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, warning others at the company to look out for calls claiming to be from top executives.

Fraudsters created a WhatsApp account with a publicly available image of Read and used it to set up a Microsoft Teams meeting that appeared to be with him and another senior WPP executive, according to the email obtained by the Guardian. During the meeting, the impostors deployed a voice clone of the executive as well as YouTube footage of them. The scammers impersonated Read off-camera using the meeting's chat window. The scam, which was unsuccessful, targeted an "agency leader", asking them to set up a new business in an attempt to solicit money and personal details.

“Fortunately the attackers were not successful,” Read wrote in the email. “We all need to be vigilant to the techniques that go beyond emails to take advantage of virtual meetings, AI and deepfakes.”

A WPP spokesperson confirmed the phishing attempt bore no fruit in a statement: “Thanks to the vigilance of our people, including the executive concerned, the incident was prevented.” WPP did not respond to questions on when the attack took place or which executives besides Read were involved.

Once primarily a concern related to online harassment, pornography and political disinformation, the [number of deepfake attacks](#) in the corporate world has surged over the past year. AI voice clones have fooled banks, [duped financial firms](#) out of millions and put cybersecurity departments on alert. In one high-profile example, an executive of the defunct digital media startup Ozy pleaded guilty to fraud and identity theft after it was reported he used voice-faking software to [impersonate a YouTube executive](#) in an attempt to fool Goldman Sachs into investing \$40m in 2021.

The attempted fraud on WPP likewise appeared to use generative AI for voice cloning, but also included simpler techniques like taking a publicly available image and using it as a contact display picture. The attack is representative of the many tools that scammers now have at their disposal to mimic legitimate corporate communications and imitate executives.

“We have seen increasing sophistication in the cyber-attacks on our colleagues, and those targeted at senior leaders in particular,” Read said in the email.

Read’s email listed a number of bullet points to look out for as red flags, including requests for passports, money transfers and any mention of a “secret acquisition, transaction or payment that no one else knows about”.

“Just because the account has my photo doesn’t mean it’s me,” Read said in the email.

WPP, a publicly traded company with a market cap of about \$11.3bn, also stated on its website that it had been dealing with fake sites using its brand name and was working with relevant authorities to stop the fraud.

“Please be aware that WPP’s name and those of its agencies have been fraudulently used by third parties - often communicating via messaging services - on unofficial websites and apps,” a pop-up message on the company’s contact page states.

Many companies are grappling with the boom of generative AI, pivoting resources toward the technology while simultaneously facing its potential harms. WPP [announced last year](#) that it was partnering with the chip-maker Nvidia to create advertisements with generative AI, touting it as a sea change in the industry.

“Generative AI is changing the world of marketing at incredible speed. This new technology will transform the way that brands create content for commercial use,” Read said in a statement last May.

In recent years, low-cost audio deepfake technology has become widely available and far more convincing. Some AI models can generate realistic imitations of a person’s voice using only a few minutes of audio, which is easily obtained from public figures, allowing scammers to create manipulated recordings of almost anyone.

The rise of deepfake audio has targeted political candidates around the world, but also crept into other less prominent targets. A school principal in Baltimore was [put on leave this year](#) over audio recordings that sounded like he was making racist and antisemitic comments, only for it to turn out to be a deepfake perpetrated by one of his colleagues. Bots have impersonated [Joe Biden](#) and former presidential candidate [Dean Phillips](#).

## At this unsettling time

We hope you appreciated this article. Before you close this tab, we want to ask if you could support the Guardian at this crucial time for journalism in the US.

**Not all journalism is the same. At the Guardian, we see it as our job not only to report the facts as we find them, but to give you the whole picture. Never sanitized or censored, our reporting provides the historical and global context necessary to fully understand the turbulent times in which we’re living.**

As we witness the erosion of democratic norms and political stability in our country - with heightened violence and division, troops on city streets, attacks on academia and science, and disregard for the rule of law - the role of the press as an engine of scrutiny, truth and accountability becomes increasingly important.

At the Guardian, we proudly platform voices of dissent, and we are fearless when it comes to investigating corruption and challenging power. We don’t have a single viewpoint, but we do have a shared set of values: humanity, curiosity and honesty guide us, and our work is rooted in solidarity with ordinary people and hope for our shared future.

Not every news organization sees its mission this way - and nor is their editorial independence as ironclad as ours. In the past year, several large US media outlets have caved to outside pressure at the behest of their corporate and billionaire owners. We are thankful the Guardian is different.

Our only financial obligation is to fund independent journalism in perpetuity: we have no ultrarich owner, no shareholders, no corporate bosses with the power to overrule or influence our editorial decisions. Reader support is what guarantees our survival and safeguards our independence - and every cent we receive is reinvested in our work.

**It has never been more urgent, or more perilous, to pursue reporting in the US that holds power to account and counters the spread of misinformation - and at the Guardian we make our journalism free and accessible to all. Can you spare just 37 seconds now to support our work and protect the free press?**

**We value whatever you can spare, but a recurring contribution makes the most impact, enabling greater investment in our most crucial, fearless journalism. As our thanks to you, we can offer you some great benefits - including seeing far fewer fundraising messages like this. We've made it very quick to set up, so we hope you'll consider it. Thank you.**

☐ Support \$5/monthly

☒ **Support \$15/monthly**

**Recommended**

Unlock **All-access digital** benefits:

- ✓ Far fewer asks for support
- ✓ Ad-free reading on all your devices
- ✓ Unlimited access to the premium Guardian app
- ✓ Exclusive newsletter for supporters, sent every week from the Guardian newsroom
- ✓ Unlimited access to our new Guardian Feast App

☐ Support once from just \$1

**Continue** →

**Remind me in November**

VISA



---

# Most viewed

---