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

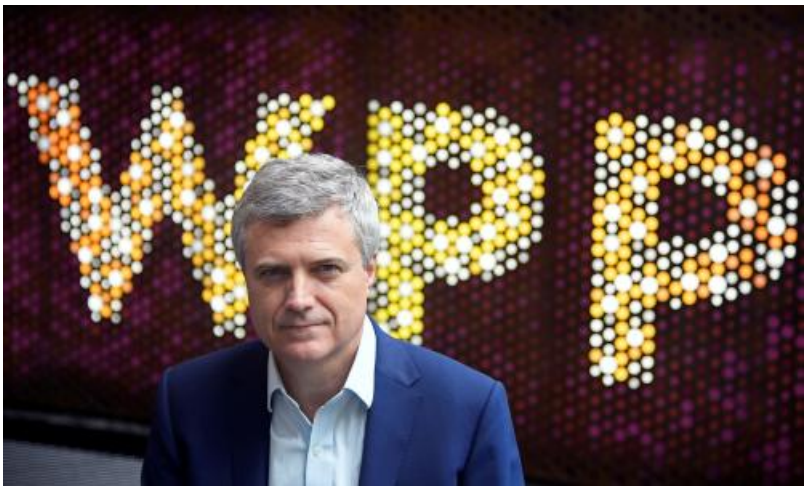
Publication Date: 2024-05-10

Author: Nick Robins-Early

Section: Technology

Tags: Technology, Artificial intelligence (AI), Deepfake, WPP, Advertising, news

Article URL: https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam



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.