

Technology

Ferrari Narrowly Dodges Deepfake Scam Simulating Deal-Hungry CEO

- Benedetto Vigna was impersonated on a call using AI software
- Large companies are being increasingly targeted with deepfakes



Benedetto Vigna *Photographer: Hollie Adams/Bloomberg*

By [Daniele Lepido](#)

July 26, 2024 at 5:28 AM CDT

It was mid-morning on a Tuesday this month when a Ferrari NV executive started receiving a bunch of unexpected messages, seemingly from the CEO.

“Hey, did you hear about the big acquisition we’re planning? I could need your help,” one of the messages purporting to be from Chief Executive Officer Benedetto Vigna read.

The WhatsApp messages seen by Bloomberg didn’t come from Vigna’s usual business mobile number. The profile picture also was different, though it

was an image of the bespectacled CEO posing in suit and tie, arms folded, in front of Ferrari's prancing-horse logo.

"Be ready to sign the Non-Disclosure Agreement our lawyer is set to send you asap," another message from the Vigna impersonator read. "Italy's market regulator and Milan stock-exchange have been already informed. Stay ready and please utmost discretion."

What happened next, according to people familiar with the episode, was one of the latest uses of deepfake tools to carry out a live phone conversation aimed at infiltrating an internationally recognized business. The Italian supercar manufacturer emerged unscathed after the executive who received the call realized something wasn't right, said the people, who asked not to be identified because of the sensitivity of the matter.

The voice impersonating Vigna was convincing – a spot-on imitation of the southern Italian accent.

The Vigna deepfaker began explaining that he was calling from a different mobile phone number because he needed to discuss something confidential – a deal that could face some China-related snags and required an unspecified currency-hedge transaction to be carried out.

The executive was shocked and started to have suspicions, according to the people. He began to pick up on the slightest of mechanical intonations that only deepened his suspicious.

"Sorry, Benedetto, but I need to identify you," the executive said. He posed a question: What was the title of the book Vigna had just recommended to him a few days earlier (it was Decalogue of Complexity: Acting, Learning and Adapting in the Incessant Becoming of the World by Alberto Felice De Toni)?

With that, the call abruptly ended. Ferrari opened an internal investigation, the people said. Representatives for the Maranello, Italy-based company declined to comment on the matter.

Why Are Deepfakes Everywhere? Can They Be Stopped?: QuickTake

Booming trend

It's not the first such attempt to impersonate a high-profile executive. In May, it was reported that Mark Read, the CEO of advertising giant WPP Plc, was also the target of an ultimately unsuccessful but similarly elaborate deepfake scam that imitated him on a Teams call.

“This year we’re seeing an increase in criminals attempting to voice clone using AI,” Rachel Tobac, CEO of cybersecurity training company SocialProof Security, said in an interview.

While these generative AI tools can create convincing deepfake images, videos and recordings, they’ve not yet proved convincing enough to cause the widespread deception that many have warned about.

However, some companies have fallen victim to fraudsters. Earlier this year, an unnamed multinational company lost HK\$200 million (\$26 million) after scammers fooled its employees in Hong Kong using deepfake technology, the South China Morning Post reported in February. The swindlers fabricated representations of the company’s chief financial officer and other people in a video call and convinced the victim to transfer money.

Other companies, such as information security outfit CyberArk, are already training their executives how to spot when they’re being scammed by bots.

Read More: [The Next Wave of Cybercrime Starts With a Deepfake Video Call](#)

“It’s just a matter of time and these AI-based deepfake sophistication tools are expected to become incredibly accurate,” Stefano Zanero, a professor of cybersecurity at Italy’s Politecnico di Milano, said in a phone interview.

– *With assistance from Lynn Doan, Jeff Stone, and Chris Miller*