

# Veteran Cybersecurity Expert Suggests We're Looking At Deepfakes The Wrong Way

*It's about the context and not the content*

CINCINNATI, OH, UNITED STATES, June 12, 2025 /EINPresswire.com/ -- As the surge in deepfakes threatens our trust in everything, veteran cybersecurity expert Neal O'Farrell warns that the focus on learning how to spot [deepfake](#) videos is only increasing the risks that we won't.

Mr. O'Farrell, a 40-year veteran of cybersecurity, one of the longest serving cybersecurity experts in the world, and the CEO of DropVault, believes we're wasting our time teaching users how to spot deepfakes.

"The quality of deepfake videos and voices is advancing so rapidly, it's nearly impossible for even experts to tell them from the real thing," said Mr. O'Farrell. "Teaching users how to spot deepfake telltales will soon be a waste of time. Our best defense is to focus less on the content and more on the context."

According to the Entrust 2025 fraud report, deepfake attacks are happening at the rate of one every five minutes with Deloitte predicting that losses to [AI](#)-assisted fraud will top \$40 billion by 2027.

Massive losses combined with the rapid erosion in consumer and business trust mean that teaching people how to spot the telltale giveaways of a deepfake video is likely to lull them into a false sense of security.

"By focusing on the context of what's being asked, users are much more likely to detect that something's just not right," said Mr O'Farrell. "It should never matter whether the video of your CEO looks real or not. What's more important is what they're asking you for."

To help users better understand the risk of deepfakes, DropVault has created a comprehensive online guide to AI crime and deepfakes that includes the following tips on spotting context telltales:

- Has the person, like your CEO, ever used a video call to make such an unusual request or ever made such a request to you at any time?
- Is the timing unusual, on a weekend or late on a Friday for example.

- Is this decision usually yours to make?
- Is there an unusual or suspicious sense of urgency?
- Is there any kind of veiled threat if you don't comply or hurry up?
- Is there a suggestion that you shouldn't double check or verify first?
- Is there any attempt to circumvent pre-agreed protocols for these kinds of requests?

The full guide to AI crime, complete with samples of incredibly realistic deepfake videos, can be found at <https://mydropvault.com/ai-crime/>

## About DropVault

DropVault brings more than 40 years of experience in cyber security and encryption to the fight against AI-assisted crime, making encrypted communications easy and accessible for everyone. Current users of DropVault range from single-person CPA firms to global airlines, banks, and wealth managers. The company has offices in Cincinnati Ohio and Dublin Ireland. For more information visit [www.mydropvault.com](http://www.mydropvault.com).

Neal O'Farrell  
DropVault LLC  
+1 513-399-6702  
[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/821141842>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.