BioID®

Spoofing Attacks

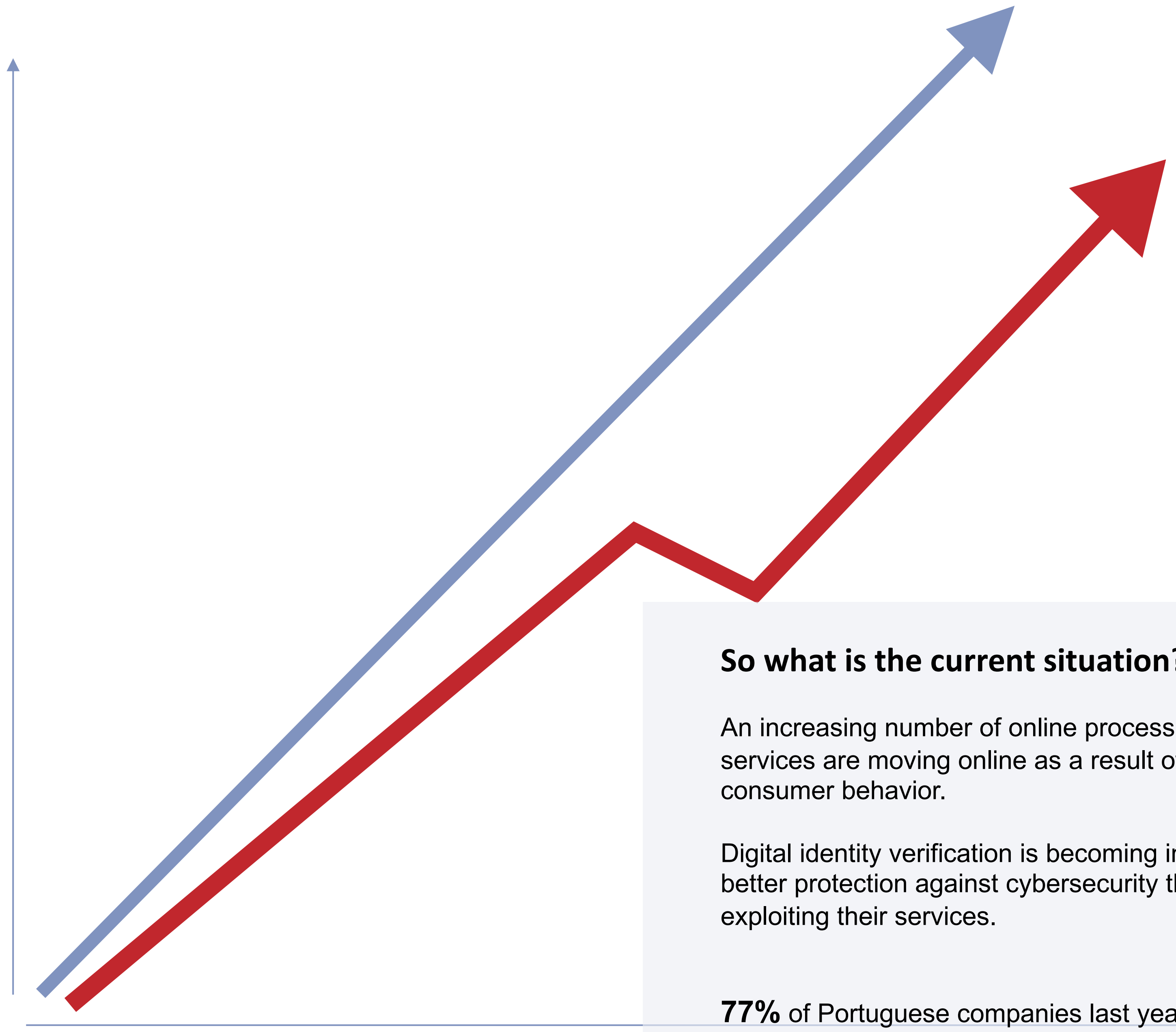
A Real Cybersecurity Threat

Business Initiation Trip Portugal
March 2023

- public -

BioID

Current Situation



So what is the current situation?

An increasing number of online processes in both private and government services are moving online as a result of globalization, COVID-19, and new consumer behavior.

Digital identity verification is becoming increasingly important in providing better protection against cybersecurity threats and preventing criminals from exploiting their services.

77% of Portuguese companies last year saw an increase in the number of disruptive cyberattacks, including the University of Lisbon (2021), telecommunications company Vodafone (2022) as well as the Portuguese Parliament (2022).

DIGITALIZATION

CYBER ATTACKS

Who is BioID?

And this is where BioID comes in:

BioID is a German biometrics company, founded in 1998 in Erlangen.

BioID originated from the German research institute “Fraunhofer IIS”.

This is where our deep research roots originate from.

We develop proprietary biometric software made in Germany, which is GDPR and ISO (30107-3) compliant.

1998

founded in Erlangen Germany

Fraunhofer IIS

25 years

of experience in multimodal biometrics

100 %

proprietary software

Information Security Management ISO 27001 Certified

BioID

What We Offer

Biometric as a Service

bioid.com/playground

BWS

We offer Biometrics as a service.

We make biometrics available just like Software as a Service (SaaS). In other words, you don't need to be a biometrics specialist to take advantage of the technology.

Our three corporate pillars are:

- **Facial Authentication**
- **PhotoVerify**
- **Liveness detection**

All technologies are consolidated in the BioID Web Service. This online service enables easy integration into any existing infrastructure via biometric API with complete anonymity of the biometric data.

You can test our biometric service for free on our demo platform, the BioID Playground.

There are many applications for BioID, such as anti-spoofing for existing facial recognition systems, (1) identity validation (2) authentication for users, (3) e-signing for fintech, online services, and eGovernment – just to name a few.

Face & Eye Recognition

Photo Matching

Liveness Detection

Spoofing Attacks

But what are spoofing attacks?

In cybersecurity, a spoofing attack is when a fraudster pretends to be someone or something else in order to gain illegitimate access or advantage.

In particular, impersonation by means of facial spoofing is by far the most-concerned cyber attack to date as digitalization is on the rise.

In this presentation, we will focus only on facial spoofing attacks.

Face spoofing attacks come in many forms.

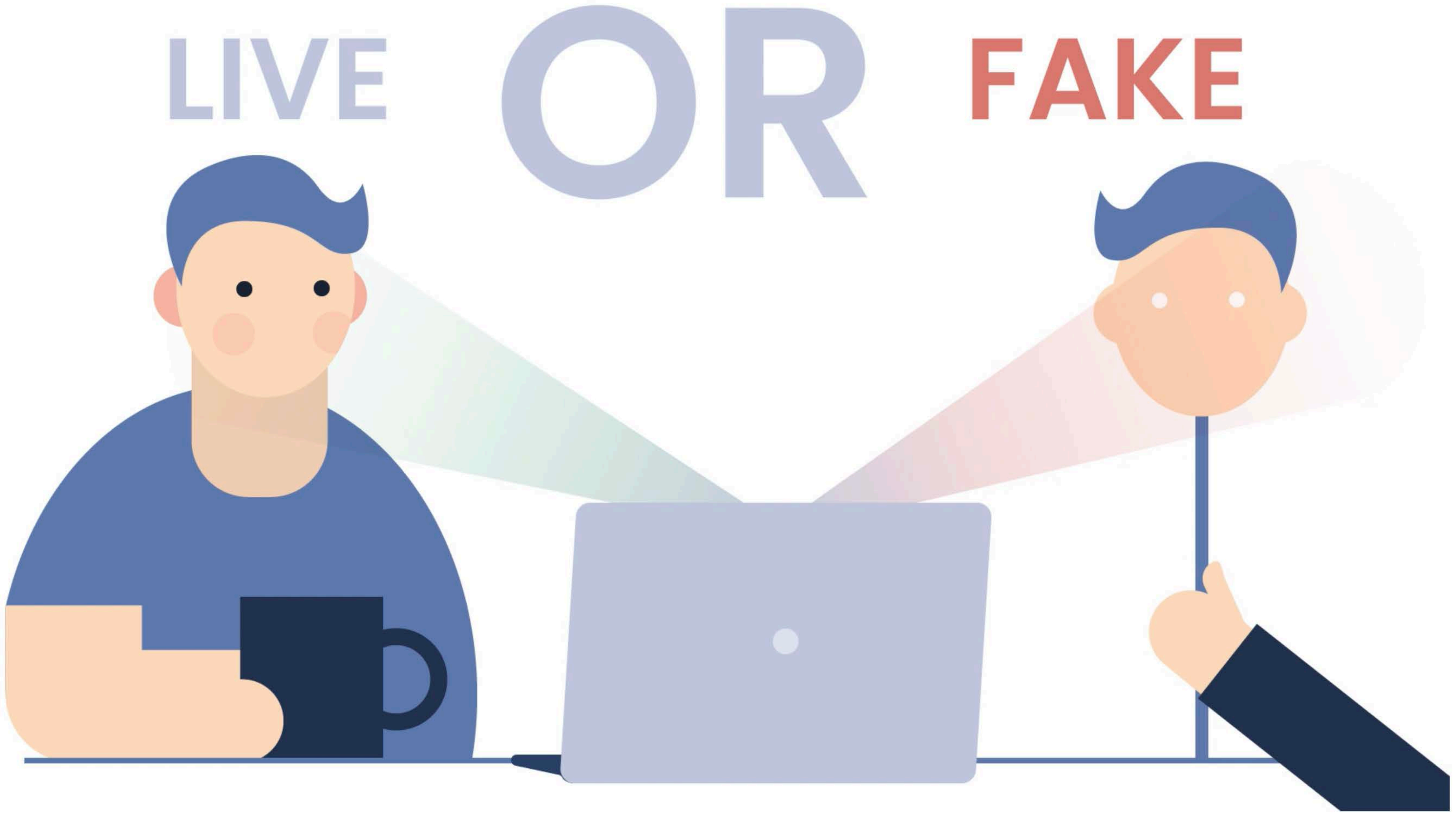
They can be conducted with various materials, in 2D and 3D, static or moving/animated

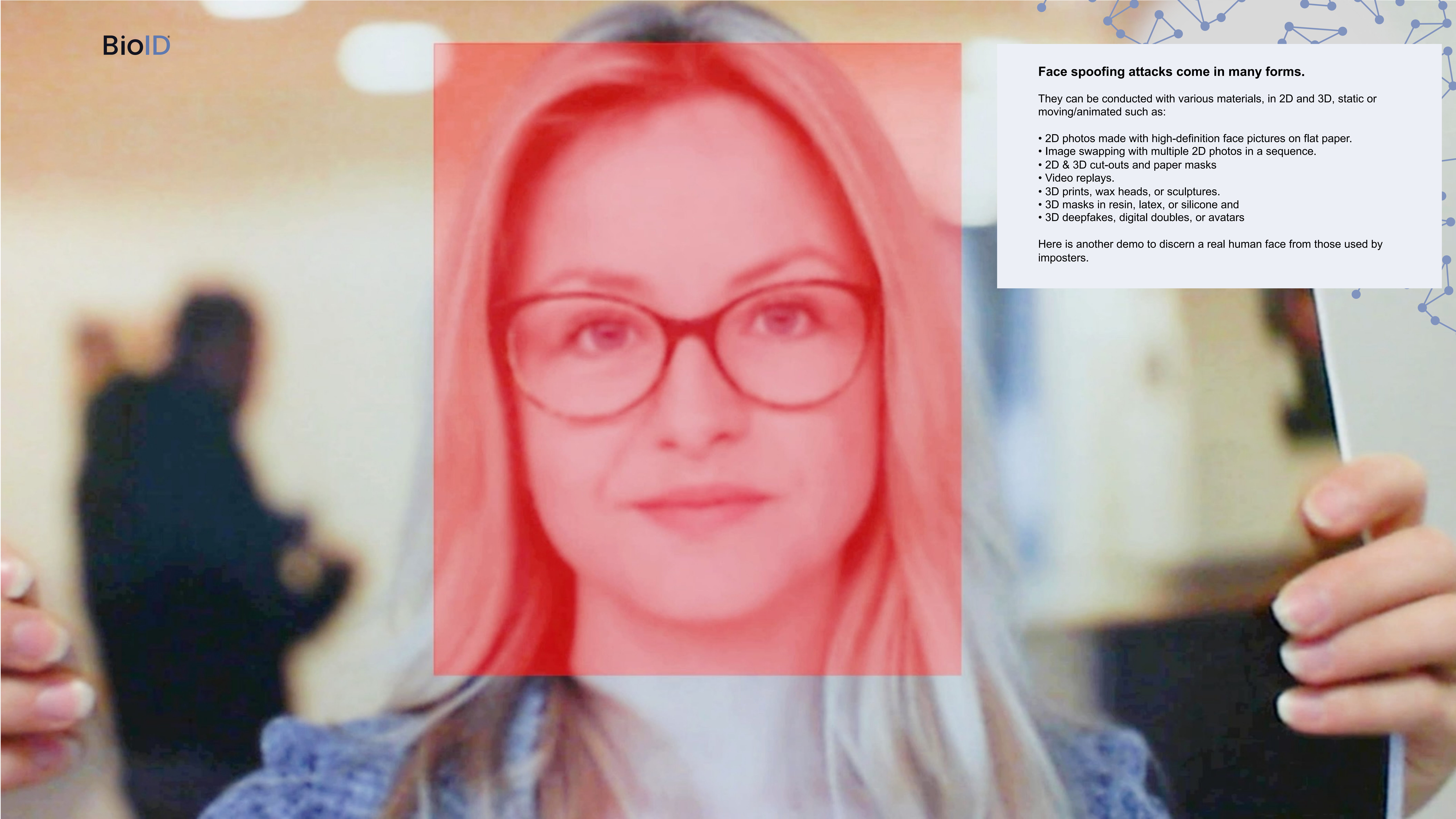
To prevent face spoofing attacks, a technique called “presentation attack detection” or simply “liveness detection” is used.

Now let’s see a video on BioID’s liveness detection in action.

RED – means fake detection and **GREEN** – means liveness detection is successful.

Meaning a live physical person has been detected.



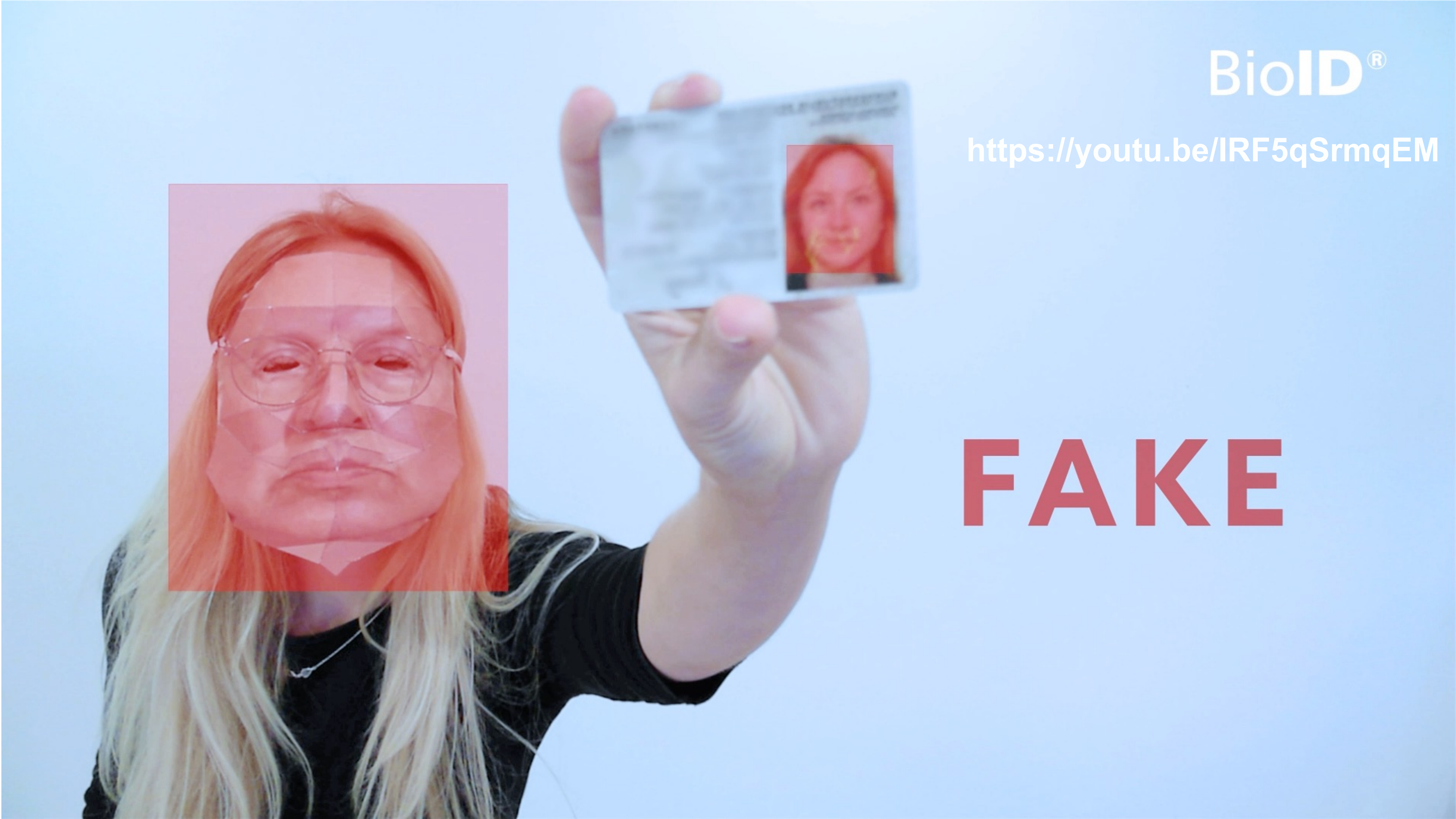


Face spoofing attacks come in many forms.

They can be conducted with various materials, in 2D and 3D, static or moving/animated such as:

- 2D photos made with high-definition face pictures on flat paper.
- Image swapping with multiple 2D photos in a sequence.
- 2D & 3D cut-outs and paper masks
- Video replays.
- 3D prints, wax heads, or sculptures.
- 3D masks in resin, latex, or silicone and
- 3D deepfakes, digital doubles, or avatars

Here is another demo to discern a real human face from those used by imposters.



BioID®

https://youtu.be/IRF5qSrmqEM

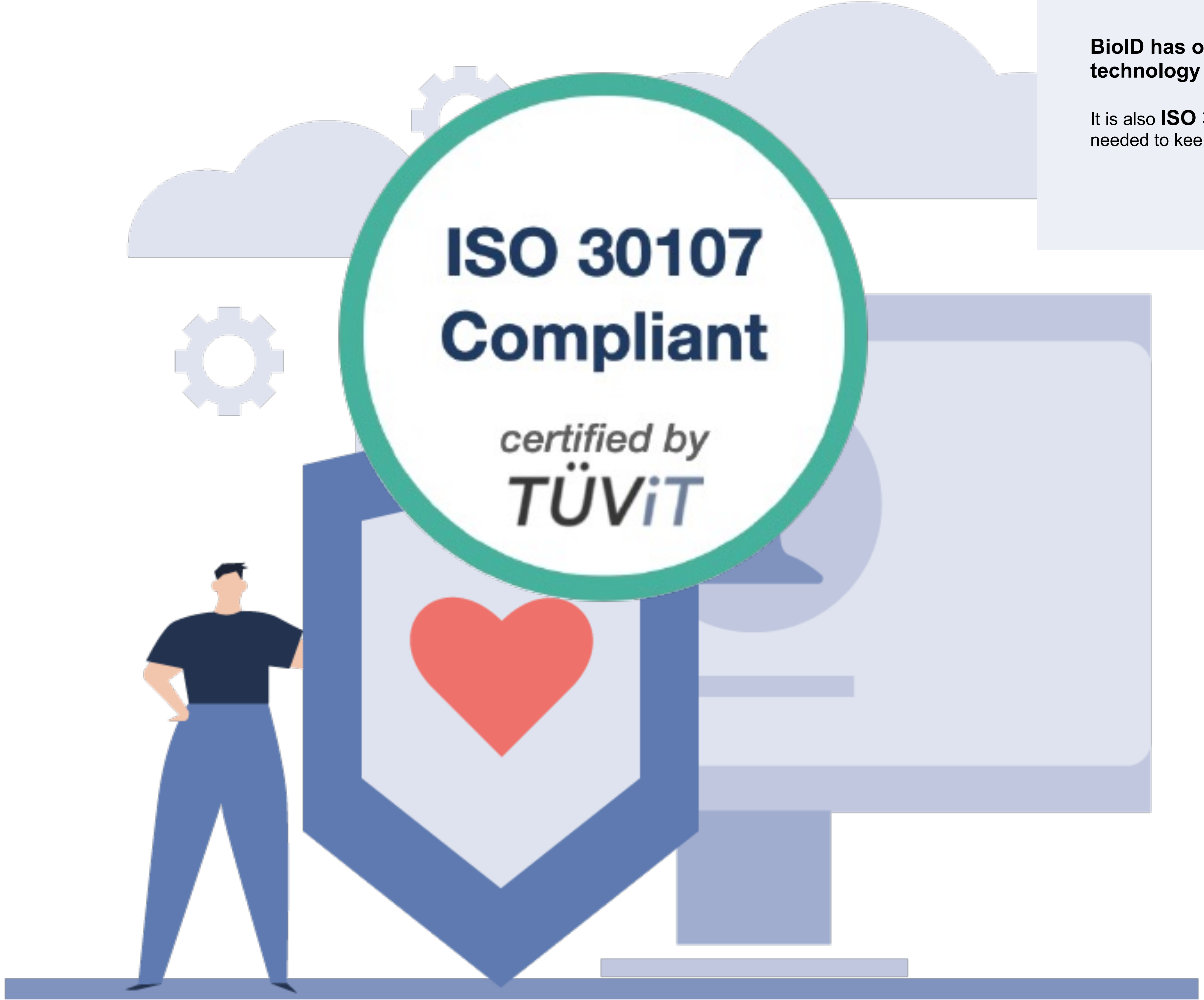
FAKE

BioID

BioID LIVENESS DETECTION

BioID has one of the world's best liveness detection technology on the market.

It is also **ISO 30107-compliant** and is being re-certified as often as needed to keep up with the evolution of the standard!



What about Deepfakes?

What about deepfakes?

What are they?
And how can we detect them?

These are well-known deepfake videos created by AI tools.

Can you believe what you see and what you hear? Can one verify the authenticity of the videos?

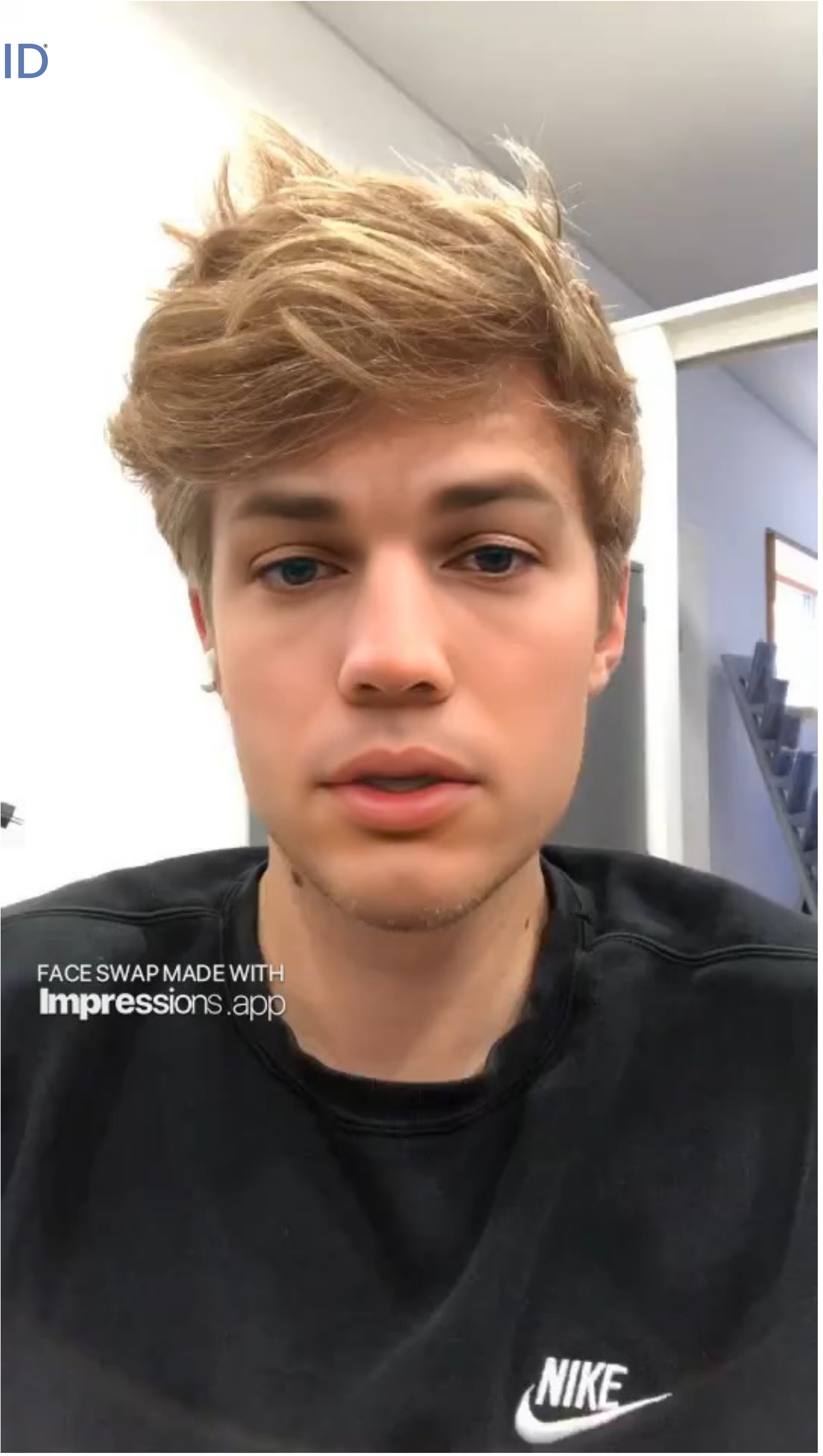
https://youtu.be/cQ54GDm1eL0

These are well-known deepfake videos created by AI tools.

Can you believe what you see and what you hear? Can one verify the authenticity of the videos?

Here is another deepfake video, where Tom Cruise is playing the guitar.

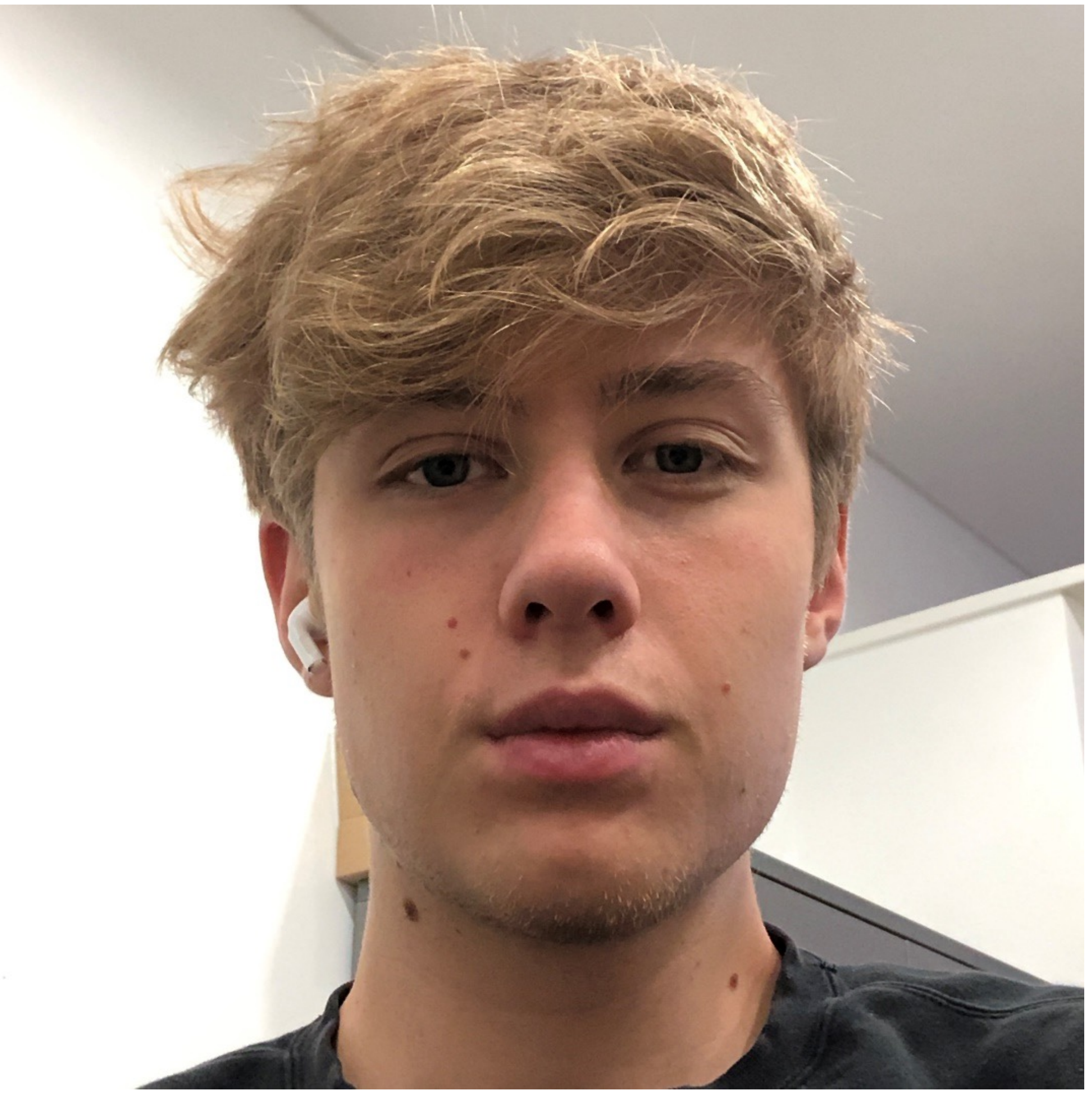
Is it real or fake? Can you tell the difference?

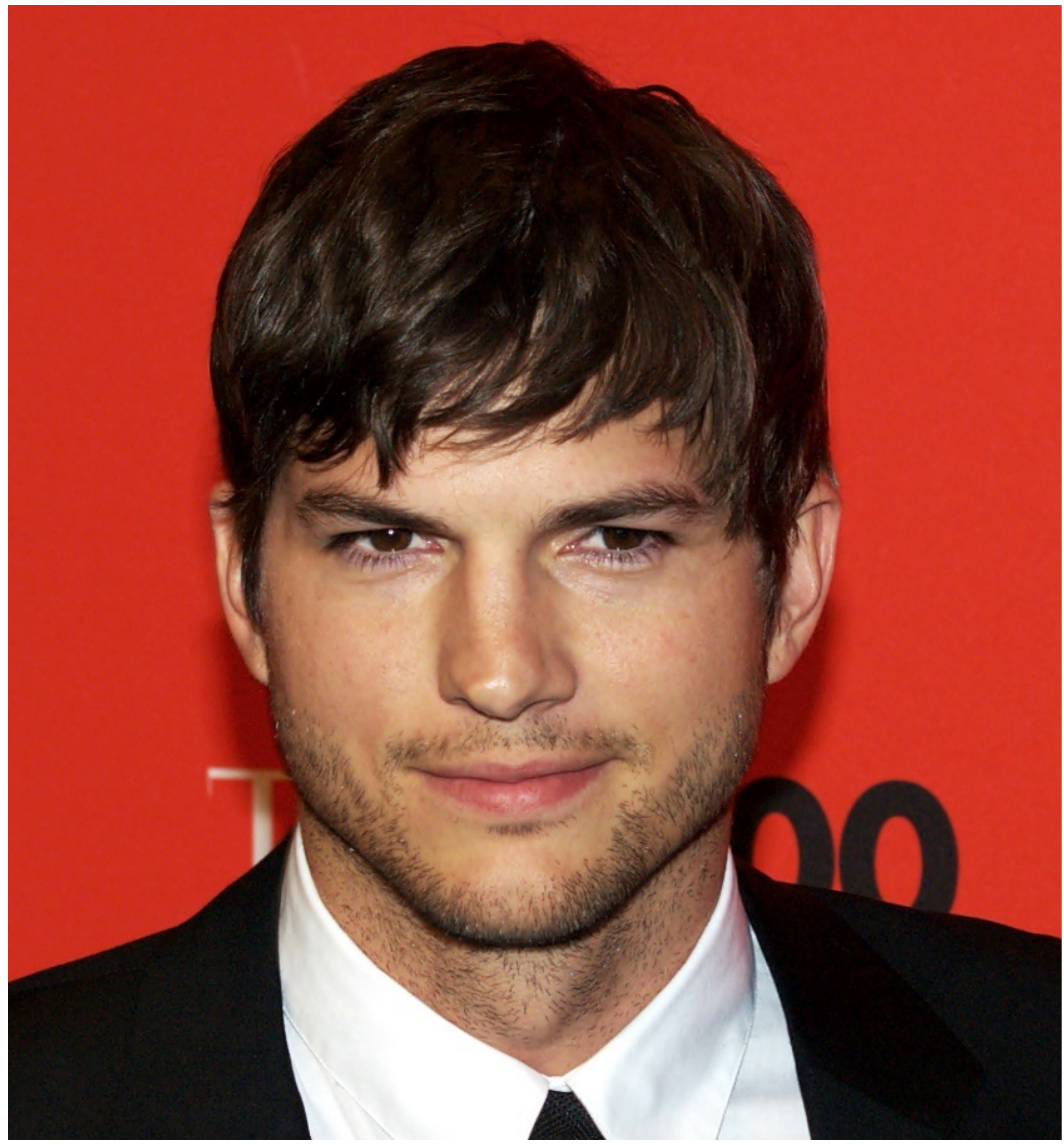


Here is a further example –

To make a deepfake video, a creator swaps one person's face and replaces it with another. Or as seen here, one can morph two faces together using a facial recognition algorithm and a deep learning computer network called a variational auto-encoder (VAE).

With such deepfakes going viral, it is clear that AI-fakes are ever-present with their surprisingly easy creation process. While surely there are benefits of deepfake technology evolving so fast | (think of the gaming or film industry), | considering the threats to security still remains extremely important!





Deepfakes Detection

Not only do deepfakes present a big risk to our cyber world in terms of the authenticity of the online content/information, but they are also posing a big challenge to our information security. So how do we prevent fraudsters from using the technology to commit unlawful criminal activities?

The truth is: Deepfake detection is a double-edged sword - because the same AI is being used not only for deepfake creation but also for its detection.

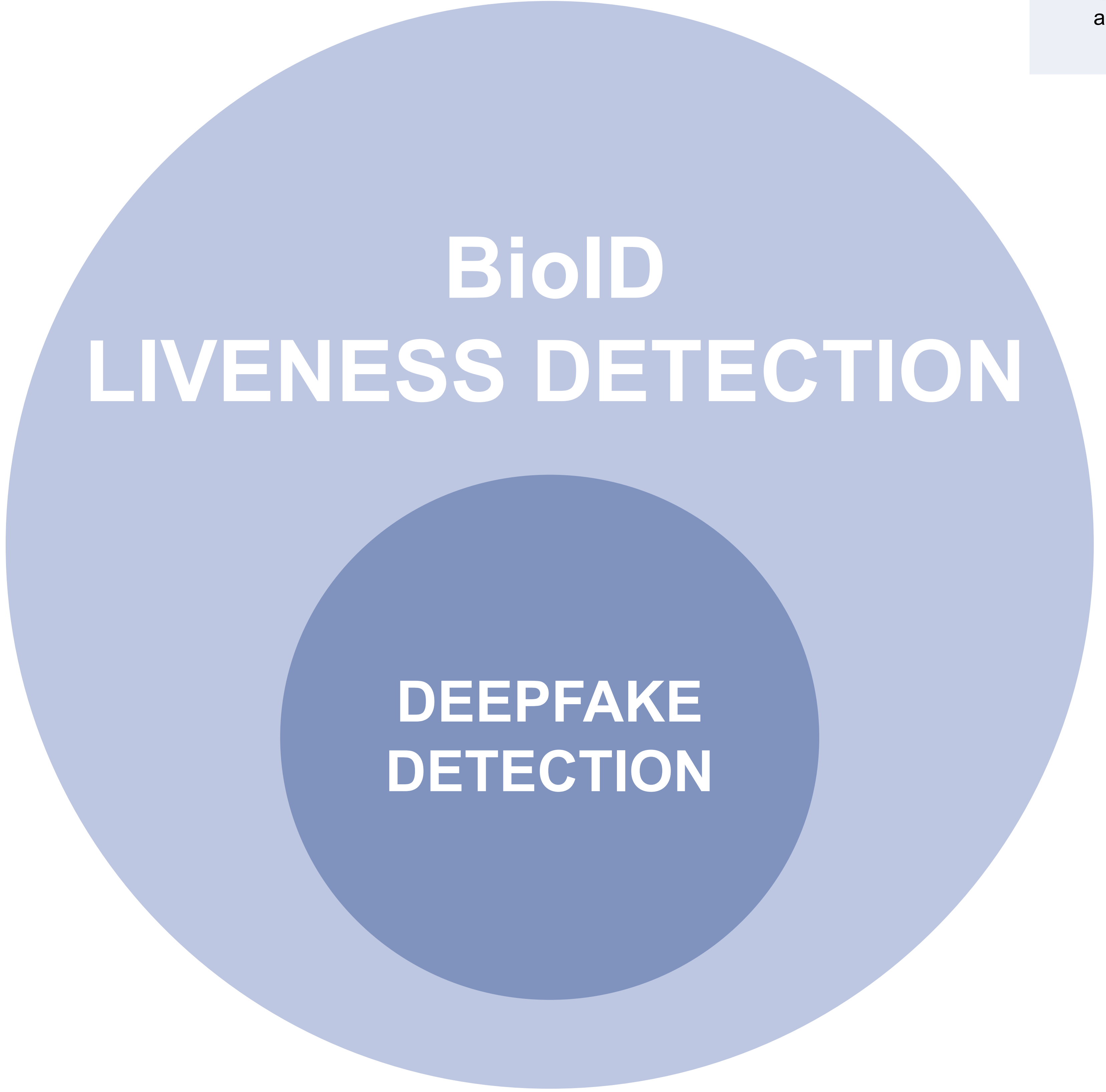
Deepfake Detection

Status Quo

BioID has been working on deepfake detection for many years now.

We can detect deepfakes with high accuracies that have been created using available AI tools such as “AvaTarify”, or “MyHeritage”.

These proven results **are being incorporated into BioID’s existing liveness detection offerings**, namely image liveness detection, as well as video liveness detection.



BioID
LIVENESS DETECTION

DEEPFAKE
DETECTION

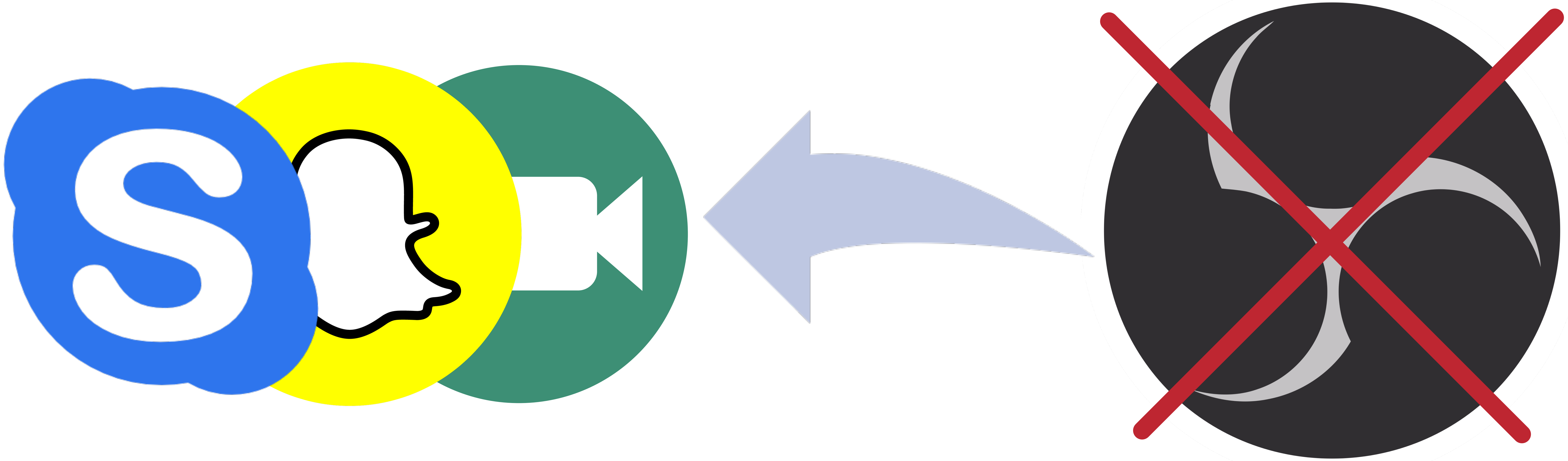
Deepfake Detection

Mitigation

The second defense strategy we employ against spoofing attacks is to detect and prevent the injection of manipulated videos/images by disabling the use of common off-the-shelf virtual cameras and webcams.

Stopping spoofing attacks is a joint effort between BioID as a biometric software provider and our customers, generally the solution providers.

Together we are securing digital identity verification with state-of-the-art liveness / deepfake detection, powered by challenge-response, and secure apps!



Disallow virtual webcam

BioID

Deepfake Detection

Mitigation

And last but not least BioID enforces the use of native mobile apps.

This is one of the most effective cybersecurity best practices.

- In principle, most secure mobile operation systems, such as iOS do not support virtual cameras
- For a web app, mobile app redirection enables powerful "Out-of-channel" verification!
- It also helps prevent man-in-the-middle attacks

Use **native** mobile app

Deepfake Detection

FAKE-ID Funded Research Project (2021-2024)

BioID

bdr. BUNDESDRUCKEREI

Fraunhofer Heinrich Hertz Institute

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

ZITiS

LKA SACHSEN-ANHALT

POLIZEI BERLIN

FHVD Fachhochschule für Verwaltung und Dienstleistung

CYBER | SEC VERBUND LAND SACHSEN-ANHALT

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Deutsche Post

Currently, the situation is that deepfakes detection is an ongoing R & D.

Apart from intensive in-house R & D, BioID is also active in the research community. In particular, BioID is proud to be a prime member of a government-funded project called FAKE-ID in Germany.

FAKE-ID is a 3-year project from 2021-2024.

As you can see, the consortium includes some of the most important stakeholders in the field, including the renowned research institute Fraunhofer, law enforcement, multiple universities as well as the German Bundesdruckerei.

BioID's primary contribution is the development of working algorithms to detect the most challenging known deepfakes to date.

With the aforementioned defense strategies, we are helping the industry to fight against cyber spoofing attacks.

Should you wish to know more about our technologies and services, please don't hesitate to contact me.

BioID

Thanks for your attention!

Questions?

Alexandra Atsüren

BioID Marketing Manager

a.atsueren@bioid.com

BioID®

www.bioid.com