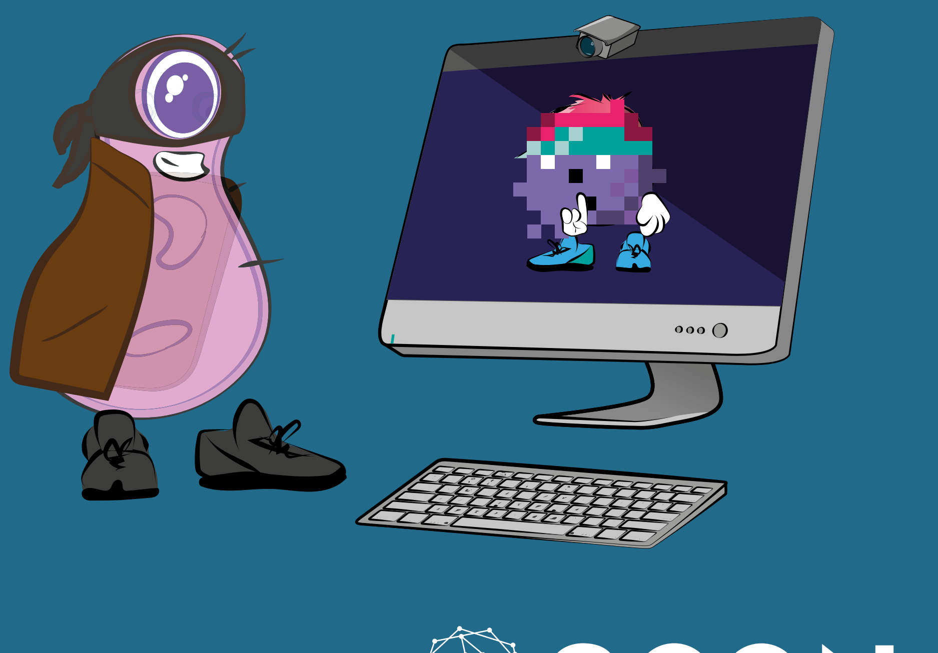
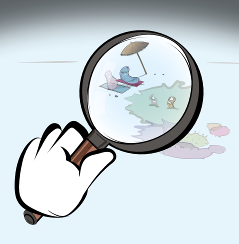
Wumbel

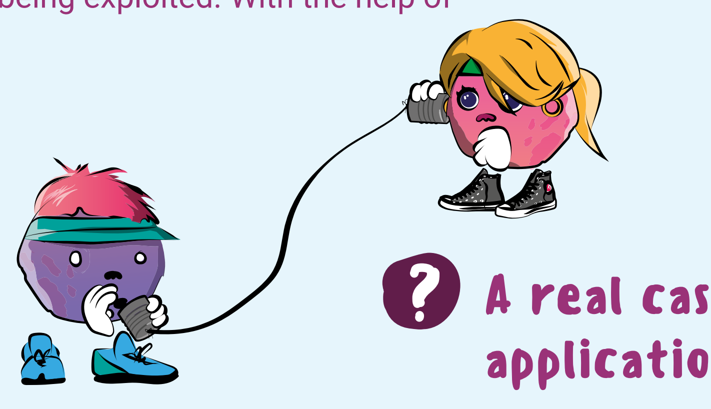
Detecting deepfakes





What you see is not always what you get.

Whether it's a video job interview, scrolling through social media, or a **virtual meeting, digital communication** has become an integral part of our everyday lives. We trust what we see and hear: **faces, voices, and body language**. But it is precisely this sense of trust that is increasingly being exploited. With the help of artificial intelligence, so-called deepfakes — manipulated audio and video recordings that appear deceptively real — are being created and used specifically to deceive. The result: **what appears to be real may in fact be pure fiction.**

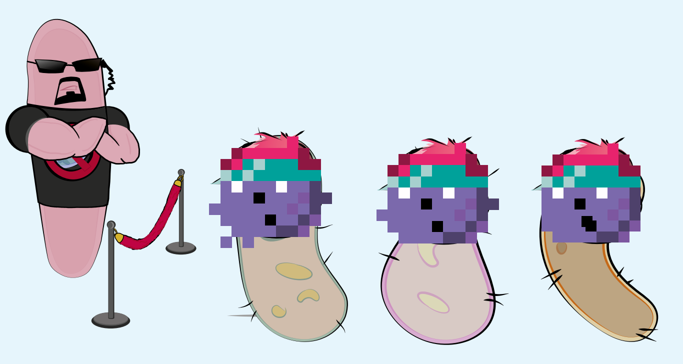


A real case from an application process:

A recent example shows how real the danger already is: During a job application process, a video interview was conducted with an apparently qualified candidate. It was only afterwards that it became apparent that the image and voice had been generated from different sources and combined using AI. **Behind this was a scam aimed at gaining access to internal company data.**

Typical areas of application for deepfakes for manipulation:

- **Job application fraud:** Criminals use fake identities to apply for remote jobs with fake video interviews, manipulated references, and cloned voices.
- **Disinformation:** Politicians, celebrities, or executives are discredited through manipulated statements with realistic-looking but fake statements or actions.
- **Blackmail & identity theft:** Personal videos are altered and used for blackmail. Deceptively real deepfake videos circulate on social networks with the aim of damaging reputations and compromising security.
- **Deception in internal meetings**: AI-generated video avatars imitate colleagues in video conferences to obtain confidential information under false pretenses.



How can you spot a deepfake?

1. **Unnatural facial expressions or speech movements:** Lip movements and audio tracks do not match exactly, or gestures appear delayed.
2. **Strange video or audio artifacts:** Distortions in the face, flickering light reflections, or fluctuating image sharpness can indicate AI manipulation.
3. **Contradictory content or sequences:** If statements do not match previous information or the context remains unclear, caution is advised.
4. **Conspicuous technical effort:** Complex video interviews with indistinctly visible interlocutors and poor sound quality may have been deliberately produced in this way.
5. **Unnaturalness:** Look out for unrealistically smooth skin and fixed gazes.
6. **Curiosity:** If unexpected questions arise in terms of number or depth, this could be an indication of espionage.

What should you do if you recognize a deepfake?

1. **Report the incident:** Inform the responsible contact persons in your organization immediately. Make a note of all relevant information and communication history.
2. **Verify sources:** Carefully check the sender and content. Use official channels and trustworthy contacts for verification.
3. **Initiate technical analysis:** IT departments or external specialists can use special tools to detect signs of manipulation.
4. **Check system protection:** Have access points checked for compromise and initiate preventive security measures.

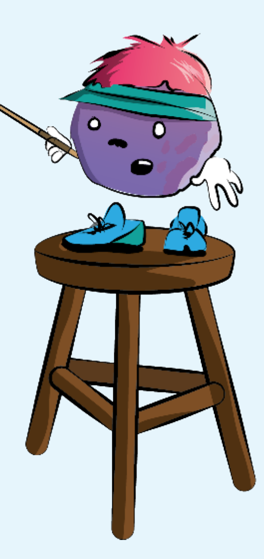
Practical tips in order to protect yourself from deepfakes

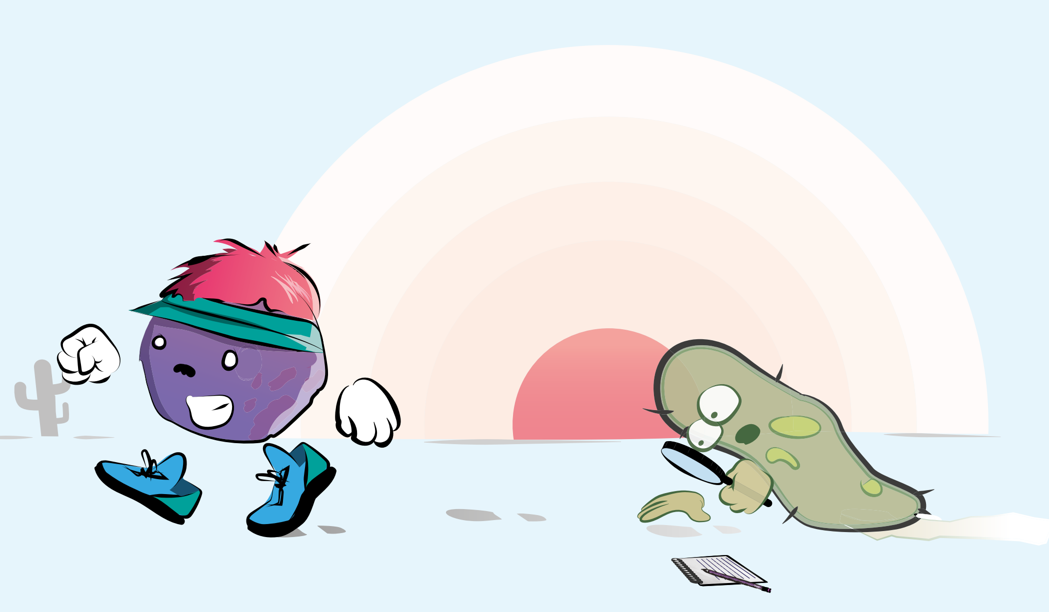
- Introduce additional authentication measures during job interviews—e.g., **live checks or follow-up verification using ID cards.**

- Use technical analysis tools to detect manipulated media **if these are approved by your company.**

- Work with clear processes for verifying the authenticity of digital content **when performing security-critical tasks.**

- Use established platforms for professional contacts and also verify identities through cross-referencing. Be skeptical **if the person cannot be found while complying with data protection regulations.**





Conclusion: Who recognizes a deepfake, can protect themselves.

Deepfakes are not a thing of the future: they are reality and deceptively realistic.

The more convincing digital fakes become, the more important it is to raise awareness and take technical and organizational precautions. Those who address the risks early on protect not only themselves, but also their organization and business contacts. This is the only way to maintain trust in digital processes.

Wumbel

S-CON GmbH & Co. KG

Podbielskistraße 386
30659 Hannover

Servicenumber: 0800 88446688
Email: office@s-con.de