Wumbel®

Deepfakes erkennen

S-CON

Was Sie sehen, ist nicht immer das, was Sie bekommen.

Ob beim **Bewerbungsgespräch** per Video, beim Scrollen durch **soziale Medien** oder im **virtuellen Meeting**, digitale Kommunikation ist aus unserem Alltag nicht mehr wegzudenken. Dabei vertrauen wir auf das, was wir sehen und hören: Gesichter, Stimmen und Körpersprache. Doch genau dieses Vertrauen wird zunehmend ausgenutzt. Mit Hilfe Künstlicher Intelligenz entstehen sogenannte, **Deepfakes manipulierte Audio- und Videoaufnahmen**, die täuschend echt wirken und gezielt zur Täuschung eingesetzt werden. **Die Folge**: Was echt erscheint, kann in Wahrheit reine Fälschung sein .

Ein realer Fall aus dem Bewerbungsverfahren:

Ein aktuelles Beispiel zeigt, wie real die Gefahr bereits ist: In einem Bewerbungsverfahren wurde ein Videointerview mit einem scheinbar qualifizierten Kandidaten geführt. Erst im Nachhinein fiel auf, dass Bild und Stimme aus verschiedenen Quellen generiert und mit KI zusammengefügt worden waren. **Im Hintergrund steckte eine Betrugsmasche mit dem Ziel, an interne Unternehmensdaten zu gelangen.**

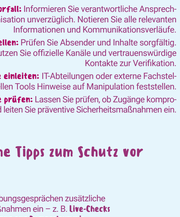
Typische Einsatzbereiche von Deepfakes für Manipulation:

- Bewerbungsbetrug: Kriminelle nutzen gefälschte Identitäten, um sich mit gefälschten Video-Interviews, manipulierten Zeugnissen und geklonten Stimmen auf Remote-Stellen zu bewerben.

- Desinformation: Politiker, Prominente oder Führungskräfte werden durch manipulierte Aussagen mit realistisch wirkenden, aber gefälschten Aussagen oder Handlungen diskreditiert.

- Erpressung & Identitätsdiebstahl: Persönliche Videos werden verändert und zur Erpressung genutzt. In sozialen Netzwerken kursieren täuschend echte Deepfake-Videos mit dem Ziel, Ruf und Sicherheit zu gefährden.

- Täuschung in internen Meetings: KI-generierte Video-Avatare imitieren Kollegen in Videokonferenzen, um vertrauliche Informationen zu erschleichen.



Wie erkennen Sie einen Deepfake?

1. Unnatürliche Mimik oder Sprachbewegungen: Lippenbewegungen und Tonspur passen nicht exakt zusammen oder Gestik wirkt verzögert.

2. Merkwürdige Video- oder Tonartefakte: Verzerrungen im Gesicht, flackernde Lichtreflexe oder wechselhafte Bildschärfe können auf KI-Manipulationen hindeuten.

3. Widersprüchliche Inhalte oder Aussage: Wenn sich Aussagen nicht mit bisherigen Informationen decken oder der Kontext unklar bleibt, ist Vorsicht geboten.

4. Auffälliger technischer Aufwand: Komplexe Videointerviews mit undeutlich sichtbaren Gesprächspartnern und schlechter Tonqualität können bewusst so produziert worden sein.

5. Unnatürlichkeit: Achten Sie auf unrealistisch glatte Haut und starre Blicke.

6. Neugier: Sollten in Anzahl oder Tiefe unerwartete Fragen kommen, könnte dies ein hinweis auf Spionage sein.

Was ist zu tun, wenn Sie einen Deepfake erkennen?

1. Melden Sie den Vorfall: Informieren Sie verantwortliche Ansprechpartner in Ihrer Organisation unverzüglich. Notieren Sie alle relevanten Informationen und Kommunikationsverläufe.

2. Verifizieren Sie Quellen: Prüfen Sie Absender und Inhalte sorgfältig. Nutzen Sie offizielle Kanäle und vertrauenswürdige Kontakte zur Verifikation.

3. Technische Analyse einleiten: IT-Abteilungen oder externe Fachstellen können mit speziellen Tools Hinweise auf Manipulation feststellen.

4. Schutz der Systeme prüfen: Lassen Sie prüfen, ob Zugänge kompromittiert wurden, und leiten Sie präventive Sicherheitsmaßnahmen ein.

Praktische Tipps zum Schutz vor Deepfakes

- Führen Sie bei Bewerbungsgesprächen zusätzliche Authentifizierungsmaßnahmen ein – z. B. **Live-Checks oder Nachverifizierungen per Personalausweis.**

- Setzen Sie technische Analyse-Tools ein, um **manipulierte Medien erkennen zu können, wenn diese durch Ihr Unternehmen genehmigt sind.**

- Arbeiten Sie bei sicherheitskritischen Aufgaben mit klaren Prozessen für die **Echtheitsprüfung digitaler Inhalte.**

- Nutzen Sie etablierte Plattformen für berufliche Kontakte und prüfen Sie Identitäten auch durch Querverweise. **Seien Sie skeptisch, wenn die Person nicht auffindbar ist unter der Einhaltung des Datenschutzes.**

Fazit: Wer Deepfakes erkennt, kann sich schützen.

Deepfakes sind keine Zukunftsmusik, sie sind Realität und täuschend realistisch.

Je überzeugender digitale Fälschungen werden, desto wichtiger wird Aufklärung und technische wie organisatorische Vorsorge. Wer sich sowohl frühzeitig als auch mit den Risiken auseinandersetzt, schützt nicht nur sich selbst, sondern auch die Organisation und die geschäftliche Kontakte. Nur so kann das Vertrauen in digitale Prozesse erhalten bleiben.

S-CON GmbH & Co. KG
Podbielskistraße 386
30659 Hannover
Servicenummer: 0800 88446688
E-Mail: office@s-con.de

S-CON