KANTON
LUZERN

Justiz- und Sicherheitsdepartement

Luzern, 26. September 2025 frs

Faktenblatt «Deepfake»

Was ist Deepfake?

Deepfake bezeichnet den Einsatz von Deep Learning und künstlicher Intelligenz, um realistische Veränderungen von Gesichtern, Stimmen und Videos zu erzeugen. Mit dieser Technologie können Gesichter oder Stimmen einer Person in Bild-, Video- oder Audioaufnahmen bearbeitet oder ersetzt werden, sodass es so aussieht, als ob diese Person verändert aussieht oder etwas gesagt oder getan hätte, was sie tatsächlich nicht getan hat.

Welche Gefahren bestehen für Sie?

Obwohl Deepfakes nicht illegal sind, können sie gegen den Datenschutz und das Urheberrecht verstossen und werden von Kriminellen oftmals für illegale Absichten genutzt. Dazu zählen:

Fake News	Die Verbreitung von Falschinformationen beispielsweise bei Meinungsbildungen und Wahlen. Deepfakes können dabei falsche Informationen als vermeintlich echt aussehen lassen aber richtige Informationen auch als falsch darstellen lassen. Dies kann zu einer Gefahr für eine Demokratie werden.
Pornographie	Es können die Gesichter von Personen (z.B. Politiker/innen) in pornographische Inhalte eingefügt werden und so die Person zu diskreditieren versuchen.
Erpressung	Mit Deepfakes lassen sich Bilder und Videos erstellen, die eine Person bei unsittlichem oder illegalem Verhalten zeigen, um diese erpressen zu können.
CEO-Scam	Cyberkriminelle ahmen die Stimme des CEO oder einer verwandten Person (Enkelkind) nach und versuchen so, Zugang zu Firmen- oder Verwaltungsdaten zu erlangen oder falsche Zahlungen auszulösen.

Wie kann ich Deepfakes erkennen?

Wer denkt, ein Deepfake vor sich zu haben, sollte auf nachfolgende Punkte achten:

Detailtreue	Da Deepfakes automatisch generiert werden, zeigen sie oft Unregelmässigkeiten bei kleinen Details z.B. Lichtreflektionen etc. Achten Sie auf diese Details.
Prüfhandlung	Zweifelt man am Gegenüber bei einem Videoanruf, fordern Sie die Person auf, etwas auszuführen (z.B. Kopfdrehen) oder auszusprechen. Bei kritischen Prozessen (z.B. Zahlungsfreigaben) eignen sich Identifikations- oder Verifikationsfragen.
Zweitkanal	Sind sie bei der Ausführung einer Anordnung unsicher, fragen Sie über einen zweiten unabhängigen Kommunikationskanal (z.B.

	Chatnachricht) nach und/oder lassen Sie sich den Auftrag so nochmals verifizieren.
Faktencheck	Bei Unsicherheit versuchen Sie die Informationen im Internet auf vertrauenswürdigen Webeseiten oder unternehmensintern unabhängig zu überprüfen

Persönliche Vorsichtsmassnahmen

Um möglichst nicht Opfer von Deepfakes zu werden, können nachfolgende Verhaltensregeln und Vorsichtsmassnahmen getroffen werden:

- Seien Sie generell zurückhaltend mit der Art und der Menge von Fotos und Videos, welche Sie online stellen. Je mehr Fotos und Videos online sind, desto grösser ist die potenzielle Gefahr des Missbrauchs.
- Kontrollieren Sie regelmässig die Privatsphäre-Einstellungen der eigenen Social-Media-Kanäle und überlegen Sie genau, mit welchen Personen Sie welche privaten Fotos und Videos teilen möchten.
- Seien Sie sich bewusst, dass auf vermeintlich privaten Messengern wie z.B. WhatsApp, die per Status geteilten Fotos und Videos, auch von unerwünschten oder unbekannten Personen eingesehen werden können, wenn Sie ihre Telefonnummer gespeichert haben. Um dieses Problem zu umgehen, kann der Status zum Beispiel nur mit ausgewählten Kontakten geteilt werden.
- Eine regelmässige Google-Rückwärtssuche von ihren eigenen Fotos kann Aufschluss darüber geben, wo diese im Netz verbreitet werden.

Opfer von Deepfakes – was tun?

Wenn Sie oder Mitarbeitende aus Ihrem Unternehmen Opfer von Deepfakes sind, empfiehlt sich nachfolgendes Vorgehen:

- Melden Sie sich umgehend beim betreffenden Seiteninhaber und verlangen Sie eine Löschung der Inhalte.
- Opfer können **Anzeige bei der Luzerner Polizei** erstatten. Seit September 2023 macht sich strafbar, wer eine fremde Identität verwendet. Wenden Sie sich dazu an den nächsten Polizeiposten.
- Opfer von Deepfakes mit intimen Inhalten können den Fall über die Seite Consensual Intimate Image Abuse melden und dort einen Fall eröffnen.

Weiterführende Informationen

Luzerner Polizei erster Kontaktort für weitere Beratung	*https://polizei.lu.ch/praevention/Cybercrime*
Deep Learning: Deep Learning einfach erklärt	*https://digitale-transformation-weiterbildung.ch/digitalisierung-lexikon/deep-learning/*
iBarry: Plattform für Internetsicherheit	*https://www.ibarry.ch/de/risiken-im-internet/deep-fake/*
PC-Tipp: Methoden, um Deepfakes zu erkennen	*https://www.pctipp.ch/praxis/sicherheit/methoden-um-deepfakes-zu-erkennen-2969643.html*
Universität Zürich: Wahrnehmung von Deepfake in der Schweizer Bevölkerung	*https://www.foeg.uzh.ch/de/research/projects/deep-fakes-wahrnehmung.html*