

Deepfakes

Präventionshinweise für Bürgerinnen und Bürger

Phänomenbeschreibung

Bei „Deepfakes“ handelt es sich um Bilder, Videos und Tonaufnahmen, die mit der Absicht erstellt oder manipuliert sind, dass sie vom Betrachtenden bzw. Hörenden als authentisch bewertet werden. Eine Form der Manipulation besteht darin, die Stimmen oder Gesichter von Personen in vorhandenen Bild- oder Videodateien durch die anderer Personen zu ersetzen. Verfälschte Inhalte können zur Begehung von Straftaten genutzt werden, beispielsweise aus betrügerischer Absicht in Videochats, für Phishing-Angriffe, Erpressung oder zur Bloßstellung von Personen – z. B. durch das Einbinden von Gesichtern in anderen Kontexten. Der Einsatz einer mittels KI-System generierten Stimme kann unter anderem für „Schockanrufe“ genutzt werden. Insgesamt ist mit einer deutlich höheren Qualität der Imitationen und so auch Täuschungsmöglichkeiten zu rechnen.

Rechtliche Einordnung

Das Veröffentlichen von Bildern oder Videos ohne Zustimmung der/des Berechtigten ist unter gewissen Umständen strafbar. Ergänzende Informationen finden Sie auf der Internetseite der Bundeszentrale für Politische Bildung [Link zur Internetseite](#).

Tipps für Betroffene

- > Keine übereilten Reaktionen (z. B. Geldzahlungen oder Überweisungen), wenn Sie selbst betroffen sind.
- > Erstellen Sie im Falle einer Sie betreffenden Veröffentlichung von den Inhalten einen oder mehrere aussagekräftige Bildschirmfotos („Screenshots“). Achten Sie darauf, dass Datum und Uhrzeit erkennbar sind. Nötigenfalls notieren Sie diese handschriftlich oder speichern das Bildschirmfoto unter Dateinamen mit Zusatz „Datum/Uhrzeit“ ab. Wenn möglich, sollte auch der Nutzer- bzw. Accountname der oder des Tatverdächtigen erkennbar sein. Die Vorgehensweise zum Erstellen eines Bildschirmfotos ist vom Gerät und genutzten System abhängig. Bei Bedarf können Hinweise zur technischen Durchführung unter Zuhilfenahme einer Internetsuchmaschine mit den Suchbegriffen „Bildschirmfoto“ oder „Screenshot“ sowie der Bezeichnung des genutzten Gerätes oder Systems zu Rate gezogen werden.
- > Melden Sie den Inhalt beim Betreiber der Internetseite. Manche Internetportale bieten hierzu schon auf der eigenen Seite eine Option im Hilfebereich an, z.B. unter „Unangemessenen Inhalt melden“. Sollte das nicht der Fall sein, wenden Sie sich an die Verantwortlichen der Internetseite (Adresse findet sich im Impressum).
- > Besteht der Verdacht einer strafbaren Handlung, erstatten Sie Anzeige bei der Polizei. Wenn sich ein Sachverhalt später als nicht strafrechtlich relevant

Kontakt:

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

herausstellt, haben Sie keinen Nachteil zu erwarten. Eine Anzeigenerstattung ist bei jeder Polizeiwache oder online möglich. Der nachfolgende Link führt zur Onlineanzeige: [Link zur Internetseite](#)

Für die Strafanzeige sind diese ergänzenden Angaben wichtig:
 Wo wurde der Beitrag veröffentlicht (vollständige Adresse/Internetadresse)?
 Welche Daten wurden von Ihnen missbräuchlich verwendet?

- > Nutzen Sie im Bedarfsfall auch die Hilfsangebote der Beratungsstellen. Im Opfer-schutzportal Nordrhein-Westfalen finden Sie entsprechende Angebote in Ihrer Nähe [Link zur Internetseite](#)

Wie Sie sich schützen können:

- > Seien Sie grundsätzlich skeptisch und bedachtsam im Internet. Skeptisch in Bezug auf dargestellte Inhalte, bedachtsam bei der Preisgabe von Daten. Sowohl ihre eigenen als auch andere Personen aus Ihrem Umfeld betreffend. So viel wie nötig und so wenig wie möglich.
- > Inhalte, die von Ihnen frei verfügbar im Internet abrufbar sind, können einem KI-System als „Trainings-Objekt“ dienen und für Fälschungen genutzt werden. Sollte sich das Veröffentlichen von Daten aufgrund beruflicher oder anderer Verpflichtungen nicht umgehen lassen, seien Sie besonders sorgsam im Umgang mit Ihren persönlichen Daten, so dass Sie als Privatperson nicht recherchierbar sind. Geben Sie in sozialen Netzwerken keine private Adresse oder auch Telefonnummern an.
- > Optimieren Sie bei Ihren privat genutzten Konten im Bereich der Sozialen Medien Ihre Privatsphäre- und Sicherheitseinstellungen.
 - Stellen Sie ein, wer Sie auf Fotos oder Beiträgen markieren darf.
 - Stellen Sie Ihr Profil auf privat. Bei öffentlichen Profilen kann jeder sehen, was Sie posten (ggf. ist das eingerichtete Konto so vorkonfiguriert).
 - Überprüfen Sie, in welchen Fällen Ihr Standort mitgesendet wird (z. B. bei veröffentlichten Fotos).
- > Haben Sie im Verlauf einer Kommunikation Zweifel an der Identität Ihres Gegenübers, beenden Sie diese und kontaktieren die fragliche Person mittels der Ihnen bekannten Erreichbarkeiten.
- > Um sich vor Täuschungen zu schützen, kann man bei bedeutungsvoller oder entscheidungsrelevanter Kommunikation (wie Geldforderungen, der Bekanntgabe wichtiger Daten) durch eine Sicherheitsabfrage (internes Wissen) einen Identitäts-Check durchführen.
- > Wählen Sie für Ihre unterschiedlichen Internetaktivitäten auch unterschiedliche und starke Passwörter. Beachten Sie in diesem Zusammenhang die Hinweise der NRW-Landeskampagne www.mach-dein-passwort-stark.de.

Kontakt:

Landeskriminalamt Nordrhein-Westfalen
 Völklinger Straße 49
 40221 Düsseldorf

Ergänzende Hinweise:

Es gibt Möglichkeiten, anhand derer die Echtheit eines Videos überprüft werden kann. Zu beachten ist hier jedoch, dass die Verlässlichkeit bei steigender Qualität gefälschter Inhalte durchaus schwankend sein kann. Auch lassen sich gewisse Merkmale oder Sicherheitsabfragen nicht in einem Echtzeitaustausch (z. B. Videoanruf) überprüfen.

Ergänzende Tipps – finden Sie auf den nachfolgenden Internetseiten. Die Links führen jeweils unmittelbar zur Themenseite

- > [Link zur Präventionsseite der polizeilichen Kriminalprävention der Länder und des Bundes](#)
- > [Link zur EU-Initiative Klicksafe](#)
- > [Link zur Internetseite des Bundesamtes für Sicherheit in der Informationstechnik](#)

Selbstverständlich können Sie sich auch jederzeit an die Kriminalkommissariate Kriminalprävention und Opferschutz beziehungsweise an die für Kriminalprävention und Opferschutz zuständigen Organisationseinheiten der Polizei in Ihrer Nähe wenden. Den Kontakt finden Sie über die Internetseite der Polizei NRW [Link zur Internetseite](#)

Ihre Ansprechstelle: