Deepfake

Präventionshinweise für Bürgerinnen und Bürger

Allgemeine Informationen

Der sensible Umgang mit eigenen und fremden Daten im Internet sowie die kritische Bewertung von digitalen Inhalten werden immer bedeutsamer. Mit Hilfe von Computerprogrammen können Kriminelle Bild-, Stimm- oder Videomanipulationen vornehmen („Deepfake“). Das Phänomen „Deepfake“ ist seit ca. 2017 bekannt. Entsprechende Computerprogramme werden stetig weiterentwickelt und verbessert. Es wird immer leichter, Bilder und Videos zu verändern und/oder Stimmen zu imitieren („Voice Cloning“). Künstlich Intelligente (KI) Systeme werden nicht nur weiterentwickelt, sondern stehen spätestens seit September 2022 in Form von sog. generativen KI-Modellen, wie z. B. ChatGPT, der breiten Öffentlichkeit zur Verfügung und können durch jedermann genutzt werden.

Phänomenbeschreibung

Bei „Deepfakes“ handelt es sich um manipulierte Bilder, Videos und auch Tonaufnahmen. Eine Form der Manipulation besteht darin, die Stimmen oder Gesichter von Personen in vorhandenen Bild- oder Videodateien durch die anderer Personen zu ersetzen. Das Ersetzen von Gesichtern nennt man „Face-Swapping“. Entsprechend künstlich generierte Inhalte sind mit steigender Qualität zum Teil schwer von echten Inhalten zu unterscheiden. Natürlich steht hier nicht immer eine missbräuchliche Nutzung im Vordergrund. Die Anwendungen können jedoch missbräuchlich zur Begehung von Straftaten verwendet werden, z. B. aus betrügerischer Absicht zur Manipulation in Videochats, für Phishing-Angriffe oder zur Bloßstellung von Personen – letzteres beispielsweise durch das Montieren von Gesichtern in anderen Kontexten. Der Einsatz einer mittels KI-System generierten Stimme kann für Betrugsdelikte im Zusammenhang mit z. B. dem sog. „Enkeltrick“ genutzt werden. Insgesamt führt die Nutzung von KI-Systemen in diesem Phänomenbereich zu einer höheren Qualität der veränderten digitalen Inhalte, was mit einer höheren Gefährdung einhergeht.

Rechtliche Einordnung

Das Veröffentlichen von Bildern oder Videos ohne Zustimmung der/des Berechtigten ist unter gewissen Umständen strafbar. Ergänzende Informationen finden Sie hier: Link zur Internetseite.

Tipps für Betroffene

> Keine übereilten Reaktionen (z. B. Geldzahlungen/Überweisungen), wenn Sie selbst betroffen sind.

> Erstellen Sie im Falle einer Sie betreffenden Veröffentlichung von den Inhalten einen oder mehrere aussagekräfte Bildschirmdrucke („Screenshots“). Achten Sie darauf, dass Datum und Uhrzeit erkennbar sind. Nötigenfalls notieren Sie diese handschriftlich oder speichern den

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Juli 2023

Bildschirmdruck 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 Bildschirmdrucks („Screenshot“) ist vom Gerät und genutzten System abhängig. Bei Bedarf können Hinweise zur technischen Durchführung unter Zuhilfenahme einer Internet-suchmaschine mit den Suchbegriffen „Bildschirmdruck“ oder „Screenshot“ sowie der Bezeichnung des genutzten Gerätes oder Systems zu Rate gezogen werden.

> Melden Sie den Inhalt auf der Internetseite. Manche Internetportale bieten Ihnen die Möglichkeit hierzu schon auf der eigenen Seite im Hilfebereich an, z. B. unter „*Unangemessenen Inhalt melden*“. Sollte dies nicht der Fall sein, wenden Sie sich an den Verantwortlichen der Internetseite (Adresse findet sich im Impressum).

> Besteht der Verdacht einer strafbaren Handlung, erstatten Sie Anzeige bei der Polizei. Auch wenn sich ein Sachverhalt später als nicht strafrechtlich relevant 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 Angaben wichtig: Wo wurde der Beitrag veröffentlicht (vollständige Adresse/Internetadresse)? Welche Daten von Ihnen wurden missbräuchlich verwendet?

> Nutzen Sie auch Hilfsangebote der Beratungsstellen. Im Opferschutzportal Nordrhein-Westfalen finden Sie entsprechende Angebote in Ihrer Nähe Link zur Internetseite

Was Sie tun können, um sich zu schützen

> Wenn Sie sich in einem Gespräch befinden, beenden Sie dieses im Zweifelsfall und kontaktieren Sie die fragliche Person unter Zuhilfenahme der Ihnen bekannten Erreichbarkeiten.

> Überlegen Sie, ob es für bestimmte Situationen (z. B. Geldforderungen) hilfreich ist, zuvor mit potenziellen Gesprächspartnerinnen und Gesprächspartnern eine Sicherheitsabfrage oder ein Kennwort zu vereinbaren.

> Eine KI lernt von Ihrer „Zielperson“ solange, bis sie diese perfekt nachahmen kann. Hierzu können Bilder, Videos oder gesprochene Texte genutzt werden. Inhalte, die von Ihnen frei verfügbar im Internet abrufbar sind, können folglich einer KI als Trainings-Objekt dienen und im weiteren Verlauf missbräuchlich verwendet werden. Seien Sie daher sensibel und sparsam im Umgang mit Ihren Daten. Achten Sie darauf, wo und welche Informationen Sie im Internet von sich veröffentlichen. Sollte sich das Veröffentlichen von Daten aufgrund beruflicher oder anderer Verpflichtungen sowie Interessen nicht umgehen lassen, seien Sie besonders

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Juli 2023

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).

> 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.

Ergänzende Hinweise und Informationen zu „Deepfakes“

Es gibt weitere Möglichkeiten, anhand derer die Echtheit eines Videos überprüft werden kann. Zu beachten ist hier jedoch, dass die Verlässlichkeit bei steigender Qualität von unechten Inhalten durchaus schwankend sein kann. Auch lassen sich gewisse Merkmale oder Sicherheitsabfragen nicht in einem Echtzeitaustausch (z. B. Videoanruf) überprüfen. Ergänzende Tipps – u. a. zur Echtheitsüberprüfung von Inhalten – finden Sie auf den nachfolgenden Internetseiten

> 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:

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Juli 2023