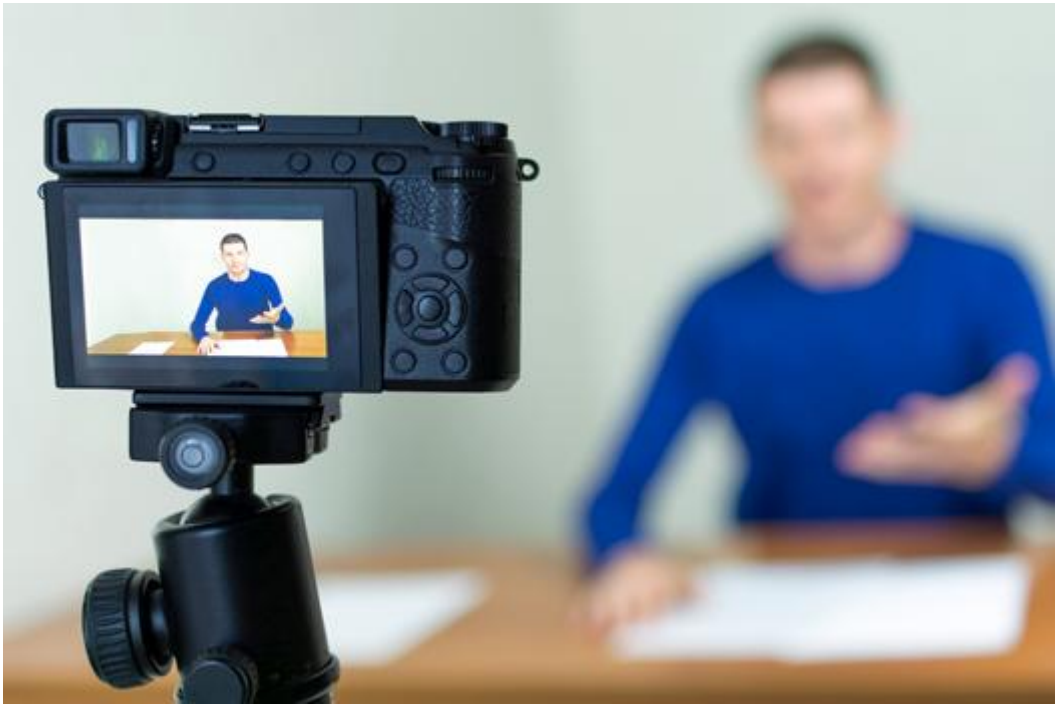
Video: Mehr Sicherheit durch Fahrerassistenzsysteme >
< Video: Hilfe bei Cybermobbing

Vorsicht vor Deep Fakes

Genau hinschauen und Quellen prüfen



Deep Fakes können großen Schaden anrichten

“President Trump is a total and complete dipshit!” – „Präsident Trump ist ein absoluter Vollidiot!” Mit dieser Beleidigung überraschte Barack Obama in einem YouTube-Video, das sich rasend schnell im Netz verbreitete. Im Verlauf des Videos wurde jedoch schnell klar: Bei der Aufnahme handelt es sich um eine Fälschung, ein so genanntes Deep Fake. Das Video stammt von Forschern der University of Washington, die auf das heikle Thema Videofälschungen aufmerksam machen wollten. Der Begriff „Deep Fake“ setzt sich aus den Worten „Deep Learning“, also der Fähigkeit künstlicher Intelligenz zu lernen, und „Fake“ (Fälschung) zusammen. Wie solche Deep Fakes entstehen und woran man sie erkennen kann, erklärt Informatiker Andreas Rössler von der TU München.

Manipulationen auch für Laien möglich

Um Deep Fakes herzustellen, braucht es nicht viel: Lediglich eine entsprechende Software, die es inzwischen frei verfügbar im Netz gibt, und möglichst viel Bild- und Videomaterial von der Person, über die man die Fehlinformationen verbreiten will. Auf Grundlage dieser Datenbasis wird die Software trainiert – und ist dann etwa in der Lage, ein Gesicht in ein anderes umzuwandeln. Bei einem Video wird dann das ursprüngliche Gesicht extrahiert und das andere eingefügt. Das alles läuft vollautomatisiert ab und ist so auch für Laien möglich. „Die Hauptarbeit für den Menschen ist, genügend Material zu sammeln“, erklärt Andreas Rössler. Den Rest erledigt die Software – die ist dann allerdings auch gut einen Tag mit der Berechnung des Endergebnisses beschäftigt.

Fälschungen werden immer besser

Wie gut das Ergebnis wird, hängt vor allem davon ab, mit wie viel Bildmaterial die Software gefüttert werden kann. „Es gibt viele Fakes, die man noch als Fälschung erkennen kann und wiederum andere, die überzeugend gemacht sind. Dabei fällt es dem Betrachter dann nicht mehr auf, dass es sich in Wirklichkeit um ein Deep Fake handelt“, erklärt Rössler. Da die Forschung und die technischen Möglichkeiten in diesem Bereich schnell voranschreiten, ist davon auszugehen, dass die Qualität der gefälschten Videos künftig immer besser wird. Rössler: „Im Bereich Virtuelle Realität wird viel geforscht – für Unternehmen ist das ein absolutes Zukunftsthema. Dabei ist es wichtig, Gesichter und Körper so bearbeiten zu können, dass sie möglichst realistisch wirken, um auch wirklich in eine virtuelle Welt eintauchen zu können. Die Ergebnisse dieser Forschung können dann aber eben auch von Betrügern zu illegalen Zwecken genutzt werden.“ Künftig wird es also zunehmend eine Herausforderung sein, echte von gefälschten Bildern und Videos zu unterscheiden. „Wir werden an den Punkt kommen, an dem Bilder und Videos nicht mehr als Beweismaterial angesehen werden können. Im Moment gelten Bilder und Videos größtenteils noch als glaubwürdig. Man nimmt sie als real hin – das wird sich ändern“, so der Experte.

Gefahren von Deep Fakes

Die Schäden, die durch Deep Fakes und andere Fälschungen verursacht werden können, sind vielfältig. So gibt es beispielsweise bereits Videos weiblicher Prominenter im Netz, deren Gesichter auf die Körper von Pornodarstellerinnen montiert wurden. Für die prominenten Frauen ist so etwas rufschädigend. Ähnliches wäre aber auch mit jeder anderen Person möglich, von der es ausreichend Bildmaterial im Netz gibt – etwa auf Social-Media-Plattformen. Denkbar wären aber auch andere Szenarien, deren Folgen kaum absehbar sind: Werden etwa Videos von Politikern gefälscht, in denen ihnen andere Aussagen in den Mund gelegt werden, könnten damit sogar Wahlen beeinflusst werden. Deep Fakes von Konzernchefs könnten wiederum für Kurseinbrüche an der Börse verantwortlich sein. „Man wird sich zunehmend Gedanken um Sicherungsmechanismen machen müssen, um die Echtheit eines Videos zu belegen, beziehungsweise eine vertrauenswürdige Quelle auszuweisen – etwa eine Art Wasserzeichen. Grundsätzlich sind frei verfügbare Informationen im Netz mit Vorsicht zu genießen, auch im Videoformat“, betont der Experte.

Andreas Rössler von der Technischen Universität München

Deep Fakes erkennen

Ein mögliches Indiz für eine Fälschung ist eine schlechte Qualität. „Fake Videos funktionieren am besten in geringer Auflösung, denn hinter der schlechten Qualität lässt sich viel verstecken, was bei besserer Auflösung sofort auffallen würde“, weiß Andreas Rössler. Achten sollte man außerdem auf die Mund- und Augenpartie, denn die beweglichen Gesichtsbereiche sind am schwierigsten zu verändern. Sieht der Mund beim Sprechen etwa seltsam oder das Blinzeln der Augen unnatürlich aus, könnte das ebenfalls ein Indiz sein. Auch die Übergänge vom Gesicht zu den Haaren, zum Hals oder zur äußeren Umgebung beziehungsweise dem Hintergrund können Hinweise auf eine Fälschung liefern, etwa wenn die Ränder ausgefranst oder unpassend wirken. Weitere Dinge, auf die man achten kann: Passt das Gesicht zum Körper? Und stimmen Gestik und Körperhaltung mit der Mimik überein? Grundsätzlich sollte auch überprüft werden: Woher stammt das Video überhaupt? Ist die Quelle nachvollziehbar? „Es liegt auch am Nutzer, den gesunden Menschenverstand einzuschalten. Genauso wie ich die Quellen von allen anderen Informationen im Netz prüfen sollte, sollte ich auch die Herkunft von Bild- und Videomaterial checken“, betont Andreas Rössler. SBa (21.12.2018)

Folgende Artikel könnten Sie auch interessieren:

- Gefährliche Online-Trends
- Bestellt und nichts geliefert
- Einsatz von Drohnen
- Die Kommunikationswelt der Zukunft
- Das vernetzte Auto
- Video: Internetkriminalität – So schütze ich mich!

Alle Artikel dieser Kategorie

Weitere Präventionsvideos

Du wirst gemobbt? Dann wehr dich dagegen!

Video: Hilfe bei Cybermobbing

Du wirst gemobbt? Dann wehr dich dagegen! Mobbing übers Netz ist...[mehr erfahren]

Mit Peter Werkmüller, Polizeiliche Beratungsstelle Düsseldorf

Video: Einbruchschutz in Gewerbeimmobilien

In diesem Video befasst sich Hauptkommissar Peter Werkmüller von...[mehr erfahren]

Konflikte im Schulalltag nachhaltig lösen

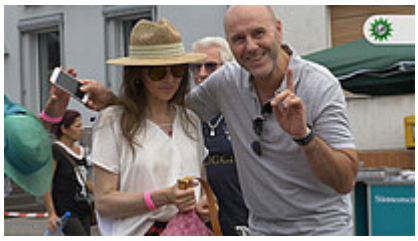
Video: Streitschlichtung in Schulen

In diesem Video wird das Streitschlichterprogramm am...[mehr erfahren]

Mit Christoph Birnstein, Automobilclub Europa (ACE)

Video: Auto winterfest machen

In diesem Video gibt Christoph Birnstein, NRW-Regionalbeauftragter...[mehr erfahren]



Erst die Opfer ablenken, dann bestehlen

Video: Taschendiebe auf Beutezug

Wer von Giovanni Alecci beklaut wird, der hat Glück. Denn er ist ein...[mehr erfahren]