Wie erkenne ich Manipulation im Netz?

Mit einfachen Tricks verfälschte Bilder, Videos und Audios entlarven

Das eigene Gesicht auf den Körper des Freundes projizieren, die Mama zu Barbie machen oder den Nachbar zu Tom Cruise? Mit Face-Swapping-Apps geht das mit nur einem Klick. Was in der Freizeit Spaß macht, wird weltweit genutzt, um gezielt Falschinformationen zu streuen. Bild-, Video- und Audio-Manipulationen dienen als Instrument, um bewusst Menschen zu beeinflussen und zu schädigen. Mit ein paar Tricks lassen sich sogenannte Deepfakes aber entlarven.

Formen der Manipulation

Um sich vor Medienmanipulationen zu schützen, sollte man die gängigsten Formen der Fälschung kennen. Face-Swapping, also das Austauschen von Gesichtern, ist aktuell die am häufigsten genutzte Methode. Eine weitere Form der Gesichtsfälschung ist das Face Reenactment. Dabei werden die Gesichtszüge einer Person verändert. Aus einem lächelnden Blick wird so zum Beispiel ein wütendes Gesicht, ob auf einem Foto oder (live) im Video. Viele Gesichtsfilter auf TikTok und Instagram nutzen diese Methode. Neben visuellen Inhalten können auch Stimmen gefälscht werden. Hier unterscheidet man zwischen Text-to-Speech (TTS) und Voice-Conversion (VC). Bei TTS liest die KI einen geschriebenen Text in der Stimme eines Opfers. So können beispielsweise Politiker in einem Video etwas ganz anderes sagen, als sie ursprünglich geäußert haben. Mit VC kann das sogar live passieren: Jemand spricht etwas ein, und am anderen Ende werden die Wörter direkt in der Stimme des Opfers ausgegeben.

Mit offenen Augen und Ohren gegen Deepfakes

Viele Manipulationen wirken verblüffend echt. Doch es gibt Indikatoren, die auf Fälschungen hindeuten. Welche das sind, hat zum Beispiel Teachtoday, eine Initiative der Deutschen Telekom, gesammelt. So soll man darauf achten, ob die Belichtung auf dem Bild oder Video stimmt oder es verwaschene Konturen gibt. Manchmal ist ein seltsamer Schatten zu sehen oder das Ohrläppchen geht schwammig in den Hintergrund über. Gefälschte Stimmen haben oft einen monotonen, metallischen Klang.“ Schenken Sie außerdem der Aussprache besondere Aufmerksamkeit, da KIs zwar die Klangfarbe einer Stimme gut erfassen, aber Probleme mit Akzenten und insbesondere Dialekten haben", empfiehlt Teachtoday. Bei gefälschten Videos bewegen sich auch die Lippen häufig nicht synchron zum Gesagten. Auf www.teachtoday.de gibt es zum Beispiel einen Entscheidungsbaum, der hilft, zu erkennen, ob es sich bei einem Video um einen Deepfake handelt oder nicht. Bei Bildern raten die Experten zudem dazu, die Bilderrückwärtssuche zu nutzen. Und immer zu hinterfragen, ob Aussagen und Handlungen zu der jeweiligen Person passen. Mit einem Blick für Details und gesundem Menschenverstand lassen sich so viele Fakes entdecken. (djd) ■