

Medietilsynets kampanje «Stopp. Tenk. Sjekk.» handler blant annet om deepfakes, som er en sterkt økende trussel:

Strand, Tormod (2023, 16. august). «Så lett er det å gjøre Abid til Einar». NRK.no. Hentet fra <https://www.nrk.no/norge/sa-lett-er-det-a-gjore-abid-til-einar-1.16510106>

Så lett er det å gjøre Abid til Einar

Med enkle grep blir Abid Raja til Einar fra Byåsen. Kunstig intelligens gjør det nå svært enkelt å lage falske videoer. – Vi risikerer at folk resignerer, og slutter å tro at noe er sant, advarer FFI-forsker Eskil Sivertsen.



FFI-forsker Eskil Sivertsen viser videoen der han overtar stemmen til Venstres Abid Raja. Foto: Helle Westrum / NRK

– Æ e trønder.

I en video laget av Medietilsynet og forskere på Forsvarets forskningsinstitutt står venstrepolitiker Abid Raja fram som trønder, fra Byåsen i Trondheim. Med tydelig trønderdialekt og en tvilsom historie om hvordan Abid ble til Einar. Stemmen i videoen tilhører FFI-forsker- og trønder- Eskil Siversten.

– Denne videoen laget vi med helt vanlig programvare som hvem som helst kan kjøpe og laste ned fra nettet, hvor man ikke har behov for noen spesielle forkunnskaper for å lage det. Det var litt av poenget vårt. Det går fint an å lage en mye bedre og overbevisende «deepfake» enn dette. Men vi ønsker å vise hvor lett det er å lage en som kanskje kan være god nok til å passere i sosiale medier på en liten mobil-skerm, sier Eskil Sivertsen.

Sivertsen har skrevet manus på filmen som er laget av Medietilsynet. NewsLab har hatt regi.



Abid Raja og Eskil Sivertsen under innspilling av videoen. Foto: NewsLab/medietilsynet

«Deepfake» er kort forklart å bruke kunstig intelligens for å lage en modell av ansiktet til en person. Deretter bytter man ut ansiktet i en eksisterende video med modellen man har laget. På samme måte kan også stemme byttes ut. Alt i et forsøk på å fåkelegge hva som er sant og ikke.

Videoen er en del av Medietilsynets kampanje, kalt «Stopp. Tenk. Sjekk».

– Det går veldig fort

Det er krig i Europa. Det er valgår i Norge. Og neste år er det valg i USA. Dette er gode grunner til å advare mot hva som kan vente oss på denne fronten, mener Eskil Sivertsen.

– Jeg tenker det er viktig, først og fremst fordi teknologien nå plutselig gjør et stort byks fremover. Det vi har sett og trodd skal komme med høy kvalitet og potensielt stort omfang, begynner nå å komme. Det går veldig fort. Da er det lurt å ligge litt i forkant av det og si «nå kommer dette».

Også det kommende kommunevalget gjør det viktig å advare, sier han.

– Den politiske debatten går høyere i valgår. Det kan være større sannsynlighet for at noen aktører kan ta i bruk denne typen virkemidler for å skape tvil om sannheten. Og ikke minst, eksistensen av «Deepfake» og lignende gir politikere og andre en anledning til å påstå at et ekte bilde, en ekte video eller et ekte lydopptak, egentlig er «fake».

Sivertsen sier også at statlige aktører som Russland kan ønske å bruke «Deepfake» som et verktøy for å spre falske nyheter i en spent sikkerhetspolitisk situasjon som vi er i nå.



100 000 «Deepfake» videoer

Så hvor mye «Deepfake» og manipulerte bilder er det egentlig der ute, i sosiale medier i Norge? Det korte svaret er: Det vet ingen. Det sier Ståle Bjørlykke Grut, som skriver doktorgrad om «Deepfakes», og har skrevet boka «Digital kildekritikk».

– Det er ikke gjort noen grundige analyser av dette i Norge. Men selskapet Sensity har fulgt den globale utviklingen en stund og antydet at det var i underkant av 100.000 deepfake-videoer på nett i slutten av 2020, og at dette doblett seg hvert halvår. Selskapet DeepMedia antar nå at rundt 500.000 lyd- og video-deepfakes vil bli delt i sosiale medier i år.



Ståle Bjørlykke Grut har skrevet bok om digital kildekritikk. Foto: Universitetet i Oslo UIO

Fra USA kommer det nå, foran neste års presidentvalg og nominasjonsprosess i det Republikanske partiet, flere eksempler på «Deepfakes». I et klipp ser det ut som om tidligere utenriksminister Hillary Clinton støtter den republikanske kandidaten Ron DeSantis. Men det hele er en «Deepfake».

Et annet eksempel fra USA er DeSantis sin kampanje som deler det som ser ut som falske bilder av Donald Trump, som klemmer Anthony Fauci, USAs svar på Espen Rostrup Nakstad under koronapandemien.

– Her brukes disse falske bildene for å sveve en politisk motstander, og for å undergrave Trump sin troverdighet i det Republikanske partiet, sier Eskil Sivertsen.



En video fra den republikanske kandidaten Ron DeSantis sin kampanje, viser bilder av Donald Trump som klemmer USAs Korona-sjef Anthony Fauci. Tre av bildene er konstruerte og kunstige ved hjelp av kunstig intelligens, AI, ifølge nyhetsorganisasjonen NPR. Faksimile: NPR

Også i Russlands angrepsskrig mot Ukraina er «Deepfake» blitt brukt. I en falsk video fra i fjor ber tilsynelatende president Volodymyr Zelenskyj ukrainske soldater om å legge ned våpnene.

Frykter at folk resignerer

Eskil Sivertsen sier kunstig intelligens og «Deepfakes» på sikt kan være en trussel mot demokratiet, også i Norge.

– Hvis nettet blir oversvømt i overveldende stor grad av falsk og villedende informasjon og falske bilder og falske videoer, så blir det veldig vanskelig for oss å finne ut hva som er sant. Hva kan vi stole på, hva kan vi ikke? Det som da kan skje, er at vi da kan resignere litt. At man trekker seg tilbake, fordi du vet at så mye av informasjonen er falsk, og du klarer ikke å vite hva du skal tro på.

– *Hvorfor er det et problem?*

– Jeg tenker hvis man resignerer, så slutter man å engasjere seg i samfunnet. Vi er avhengig av politisk engasjement og en opplyst befolkning for å ha et demokrati. Og hvis vi ikke har en befolkning som er i stand til å delta i en offentlig samtale basert på hva som faktisk skjer rundt oss, så vil jo det bli en svekkelse av demokratiet.

Sivertsen sier redaktørstyrte medier nå er viktigere enn før, fordi de kan avdekke hva som er sant, og at de i en situasjon er det florerer med falske videoer og bilder vil være det Sivertsen kaller en magnetisk nordpol for hva som er sant og ikke.

– Men det forutsetter jo at redaktørstyrte medier beholder sin troverdighet, og ikke mister tillit, sier han.

Hvor lett tilgjengelig er egentlig denne teknologien idag? Utviklingen går fort, sier Ståle Bjørlykke Grut.

– De mest avanserte og troverdige løsningene for video krever fortsatt en del ressurser og er forbeholdt film-industrien eller eksperter med bakgrunn derfra. Overraskende gode varianter, spesielt når det kommer til bilder, er også tilgjengelig gjennom apper som kan kjøres på en vanlig datamaskin eller mobiltelefon.

– *Hvorfor har denne teknologien blitt så lett tilgjengelig?*

– I hovedsak dreier det seg om økt datakraft, i datamaskiner, mobiltelefoner og skyløsninger. Disse gjør det mulig å gjøre krevende operasjoner på kortere tid og ved bruk av mindre maskinvare, sier Bjørlykke Grut.

Tips til hva du skal se etter

Eskil Sivertsen sier vi alle på internett og sosiale medier har et ansvar for å ikke dele falske nyheter og «Deepfakes».

Men det er enkelt for han å si, for hvordan finner du som leser ut om en video er falsk eller ikke?

Ståle Bjørlykke Grut deler noen tips om hva du skal se etter:

- Å få inn en sunn skepsis til bilder og videoer som har oppsiktsvekkende innhold som del av ryggmargsrefleksen er kanskje det viktigste. Spesielt om du ikke kjenner avsenderen fra før.
- Deretter kan man begynne å se på detaljer i bildet og videoen. Er det noe som ikke stemmer i overganger mellom forgrunn og bakgrunn? Ser konturene rundt ansiktet og hendene unaturlige ut? Er bakgrunnen uskarp og detaljer vanskelig å se? Da kan det være grunn til mistanke.
- Utfordringen er at teknologien blir stadig bedre, og at tekniske løsninger for å avsløre at noe er laget av AI er mangelfulle eller ikke fins i det hele tatt. Derfor er det lurt å være kildekritisk samtidig som man holder seg noenlunde oppdatert på den teknologiske utviklingen.

Medietilsynet mener nordmenns kildekritiske sans er viktigere enn noen gang, for å hindre «»Deepfake«» og falske nyheter i å spre seg i Norge. Så hvordan står det til med den kritiske sansen?

– Vi vet fra forrige undersøkelse Medietilsynet gjorde om nordmenns kritiske medieforståelse at omrent halvparten sjekker med flere ulike kilder, dersom de kommer over informasjon de er usikre på om er sann. Det er jo ganske bra, men vi ønsker jo at enda flere skal bli mer kildekritiske. Det sier direktør i Medietilsynet, Mari Velsand.

Økokrim advarer mot at deepfakes i økende grad brukes i svindel:

Farestvedt, Ingrid Bjørndal og Elgaaen, Vilde (2024, 7. februar). «Økokrim advarer mot deepfake-svindel: – Svært troverdig». VG.no. Hentet fra <https://www.vg.no/nyheter/i/4oMKI9/oekokrim-advarer-mot-deepfake-svindel>



En finansmann i Hongkong ble nylig frasvindlet over 270 millioner norske kroner under et videomøte. Dette bildet er fra 2020. Foto: JEROME FAVRE / EPA / NTB

Økokrim advarer mot deepfake-svindel: – Svært troverdig

Kunstig intelligens gir svindlere nytt spillerom.

Ingrid Bjørndal Farestvedt og Vilde Elgaaen

Onsdag 7. februar kl. 14:39

Nå advarer Økokrim mot en ny type svindel som bruker deepfake-teknologi til å manipulere bilder, video og lyd.

Målet er å lure folk til å gi fra seg sensitiv informasjon eller overføre penger, skriver de i en pressemelding.

I helgen meldte CNN om en finansmann i Hongkong som ble utsatt for et slikt svindelangrep:

- Under et videomøte med personer han trodde var kollegaer, ble mannen lurt til å overføre svimlende summer – tilsvarende over 271 millioner norske kroner.
- Det viste seg i ettertid at møtet var iscenesatt av svindlere som hadde manipulert video og lyd ved hjelp av deepfake-teknologi.

Teknologien gjør det mulig å utgi seg for å være en annen person, understreker Økokrim:

– Svindlerne bruker kunstig intelligens i kombinasjon med sosial manipulasjon for å skape tillit hos offeret, sier avdelingsdirektør Lone Charlotte Pettersen.

MrBeast har også advart sine følgere mot deepfake-videoer:



MrBeast advarer

Rampelys · 4. okt. 2023

0:44

Bilde av video av MrBeast. Kan ikke spilles av på eksamen.

Økokrim tror denne typen svindel vil øke.

– Kriminelle har begynt å ta i bruk deepfake-teknologi, noe som gjør angrepene svært troverdige. Det er ingen grunn til å tro at vi er mindre utsatt for slike bedragerier her enn i andre land, advarer Pettersen.

Denne artikkelen er laget ved hjelp av AI-verktøy fra Anthropic, og kvalitetssikret av VGs journalister.