Nieuwe vorm van oplichting: stemmen klonen met behulp van AI

Een nepspeech van de minister-president, gezichts- en stemvervorming in films en gekke filters op social media. AI geruime tijd kunnen we met behulp van AI-technologie bestaand beeld en geluid digitaal manipuleren. De technologie wordt alsmaar beter, waardoor de manipulaties amper van echt te onderscheiden zijn. Een ontwikkeling waar mensen met vervelende of illegale bedoelingen helaas ook steeds meer gebruik van maken.

Het gebruik van deepfake-video's om nepnieuws te verspreiden, mensen te kwetsen of op te lichten is al wat langer bekend. Het kopiëren van stemmen, voice cloning, met het doel mensen op te lichten zien we nu ook steeds vaker voorkomen.

Deepfakes en voice clones, wat zijn het?

Deepfake is een combinatie van de Engelse termen *deep learning* en *fake* (nep). Deepfakes zijn digitale manipulaties van beeld en video, waarbij artifical intelligence-technologie gebruikt wordt om originele beelden te veranderen of zelfs volledig neppe beelden te creëren. Een afgeleide daarvan is de *audiofake* of *voice clone*. De term zegt het al, dit is een manipulatie van een audio-opname, zoals echte stemopnames of geluidsfragmenten, waar ook AI voor wordt gebruikt. Het wordt ook wel *voice cloning* genoemd.

Zowel deepfakes als voice clones worden op allerlei creatieve manieren ingezet. Denk aan het creëren van special effects voor films of videogames. Maar ook voor het tot leven wekken van oude foto's en creëren van gekke filters op social media. De technologie wordt alsmaar beter en maakt hyperrealistische tegenwoordig van dusdanig goede kwaliteit, dat acteurs in Hollywood zich zorgen maken dat zij door AI op een gegeven moment overbodig worden.

Hoe gebruiken criminelen voice cloning-technologie?

Software en apps om stemmen te kopiëren zijn makkelijk beschikbaar en te gebruiken, waardoor iedereen zo'n digitale manipulatie kan maken. Criminelen zetten deze steeds vaker in om mensen op te lichten en geld afhandig te maken. Het enige wat ze hiervoor nodig hebben is een kort fragment van iemands stem, een paar seconden is genoeg. Deze vinden ze op social media of nemen ze op tijdens een telefoongesprek.

Hoe herken je een nepstem?

De eerste nepstemmen waren met het blote oor te herkennen. Denk aan stemmen die niet helemaal als het origineel klonken of haperden. Maar AI-technologie ontwikkelt zich razendsnel, waardoor het herkennen van een nepstem steeds moeilijker wordt. Cybercriminelen maken hier voor fraude en oplichting steeds meer gebruik van. Bijvoorbeeld door iemands stem na te maken, om vervolgens

Bronnen:

- https://veiliginternetten.nl/thema/social-media/zijn-deepfakes-gevaarlijk/
- https://veiliginternetten.nl/thema/social-media/wat-zijn-deepfakes/
- https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
- https://www.scamadviser.com/articles/how-scammers-are-using-voice-clones-to-scam-millions

telefonisch mensen te overtuigen om geld over te maken. Iedereen kan hier helaas de dupe van worden: een bekende Nederlander, de directeur van een groot bedrijf, maar ook je vader of moeder.

Een eng idee, en helemaal niet raar als deze ontwikkelingen mensen onzeker maken over dingen die ze horen en zien in de digitale wereld. Want wat is nog echt en wat is nep? Het is geen reden om bang te worden, wel om kritisch te blijven. Net als in de offline wereld, zijn vervelende situaties, zoals diefstal of grensoverschrijdend gedrag, online niet uit te sluiten. En ondanks dat nepstemmen steeds moeilijker te herkennen zijn, zijn er een enkele vuistregels waarmee we het risico op vervelende situaties kunnen verkleinen.

Hier kun je op letten

De allerbelangrijkste tip: maak nooit zomaar geld over, zelfs niet aan een goede bekende. Belt een bekende en vraagt diegene je om direct geld naar ze over te maken? Wees dan alert. Hang op, bel diegene terug op het nummer dat je van ze hebt opgeslagen en vraag door. Blijkt deze persoon jou niet gebeld te hebben, schakel dan de politie in.

Verder zijn er een aantal signalen waar je op kan letten.

- De beller vraagt je om snel geld over te maken.
- De beller vraagt om geld te sturen via lastig te traceren methoden, zoals cryptocurrency of cadeaubonnen.
- Het verhaal van de beller is inconsistent.
- Luister goed naar de achtergrondgeluiden. Als de beller een goede stem heeft met weinig tot geen waarneembare achtergrondgeluiden, hang dan op.
- Als het verhaal van de beller inconsistent is, hoe klein ook, ga dan voorzichtig te werk.
- Ga niet te veel met de beller in gesprek, want dit kan ze de kans geven om ook jouw stem te klonen.

Vertrouw je het niet? Hang dan op en bel de persoon terug op het nummer dat je van ze hebt opgeslagen. Nemen ze niet op? Probeer dan via een familielid of vriend met hen in contact te komen.

Beperk het online delen van persoonlijke informatie

Voor heel veel verschillende manieren van online criminaliteit maken cybercriminelen gebruik van persoonlijke informatie die ze online kunnen vinden. Denk aan informatie over je leeftijd, woonplaats en interesses, maar ook foto’s en filmpjes. Zet social media-accounts altijd op privé en vermijd het delen van persoonlijke gegevens op sociale media.

Bronnen:

- https://veiliginternetten.nl/thema/social-media/zijn-deepfakes-gevaarlijk/
- https://veiliginternetten.nl/thema/social-media/wat-zijn-deepfakes/
- https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
- https://www.scamadviser.com/articles/how-scammers-are-using-voice-clones-to-scam-millions