Voice cloning is een nieuwe technologie die met artificiële intelligentie (AI) iemands stem kan kopiëren. Cybercriminelen gebruiken het om mensen telefonisch op te lichten. Hoe werkt het? En wat kan je ertegen doen?

Met kunstmatige intelligentie kan een computerprogramma iemands stem namaken. Het enige wat hiervoor nodig is, is een korte opname van de stem van de persoon. De techniek is ontwikkeld om spraak beter te herkennen, audioboeken in te spreken en voor films. Maar omdat de nagebootste stem zo erg lijkt op de échte stem, kunnen mensen makkelijk voor de gek worden gehouden. Nog gevaarlijker is dat je een gekloonde stem dingen kan laten zeggen die die persoon nooit heeft gezegd. Dat weten criminelen natuurlijk ook: zij maken handig misbruik.

Criminelen en voice cloning

Criminelen gebruiken *voice cloning* voor oplichting en fraude. Bijvoorbeeld om nepnieuws te maken of om mensen geld afhandig te maken. Oplichters kopiëren de stem van een vriend of familielid. Met die gekloonde stem bellen ze hun slachtoffer op en vragen om geld over te maken of om persoonlijke gegevens te delen.

Voice cloning is in opmars

Buitenlandse media hebben de afgelopen jaren bericht over mensen die geld zijn verloren aan oplichters die stemmen van hun familieleden hadden nagemaakt. In Canada zijn acht mensen in drie dagen tijd bestolen voor omgerekend 135.000 euro. Sinds kort zien we deze vorm van cybercriminaliteit ook in Nederland. Uit onderzoek van de Rijksoverheid blijkt zelfs dat 60 procent van de Nederlanders denkt dat een gekloonde stem van een bekende echt is. En maar 4 procent van de Nederlanders kan met zekerheid een gekloond stemfragment herkennen.

Dit zijn de gevaren

Oplichters proberen vertrouwen te winnen door zich in een telefoongesprek voor te doen als een familielid, vriend of zakenrelatie. Als je even niet oplet, kan je onbedoeld persoonlijke informatie delen. Bijvoorbeeld een burgerservicenummer (BSN), geboortedatum en -plaats, pincode of creditcardnummer. Met deze gegevens kunnen criminelen identiteitsfraude plegen.

Hier moet je op letten

Online criminelen maken handig misbruik van menselijke eigenschappen zoals behulpzaamheid en beleefdheid. Manon den Dunnen, Strategisch Specialist Digitaal bij de politie: “Een makkelijke vuistregel is, zodra je een beslissing moet nemen die onomkeerbaar is zoals het overmaken van geld of het delen van vertrouwelijke informatie, dat je dan een stapje terug doet en de informatie op andere wijze probeert te verifiëren. Ook als je die persoon goed kent. Dat voelt misschien onbeleefd of onprettig, maar mensen zullen dit steeds normaler gaan vinden.”

Twijfel je of een gesprek echt is? Hang dan op en bel terug op het officiële telefoonnummer. Stel vragen over iets wat alleen die persoon kan weten. Hou er rekening mee dat oplichters op internet (social media) makkelijk informatie over je te weten kunnen komen. Meer tips lees je hier: laatjenietinterneppen.nl en op de website Veilig internetten.nl.

Slachtoffer geworden?

Het is heel normaal dat je geschrokken bent als je toch bent opgelicht. Of dat je je schaamt, omdat je erin getrapt bent. Nergens voor nodig. Het is belangrijk om zo snel mogelijk actie te ondernemen. Op een rijtje:

- Blokkeer direct al je bankpassen en creditcards. Kijk hier op de website van de politie. Ook de website van de Consumentenbond bevat een lijst van telefoonnummers van alle banken om je pas te blokkeren.
- Doe meteen aangifte bij de politie, bijvoorbeeld via de website van de politie of door te bellen naar 0900-8844.
- Informeer de Fraudehelpdesk via de website of door te bellen naar 088-7867372.
- Neem geen risico en meldt dit bij het Centraal Meldpunt Identiteitsfraude. Op deze website vind je een meldingsformulier. Je kunt ook bellen: het telefoonnummer is 088 – 900 10 00.

Tags:

- Veilig online