Alarm om nieuwe criminele truc met deepfake: 'Hackers kopiëren je gezicht en plunderen je bankrekening'; ING neemt maatregelen

De Telegraaf.nl

7 april 2024 zondag 3:00 AM GMT

Section: LIFESTYLE; FRONTPAGE; LIFESTYLE/WETENSCHAP

Length: 861 words

Byline: Sven Rietkerk

Body

Cybercriminelen hebben een nieuwe manier gevonden om geld te stelen. Ze kunnen gezichten van telefoongebruikers stelen en zo toegang krijgen tot hun bankrekening om die te plunderen. ING waarschuwt klanten en neemt zelf 'zichtbare en onzichtbare maatregelen' om dit te voorkomen. „Mensen kunnen jouw gezicht stelen en namaken", waarschuwt Ot van Daalen, advocaat root legal & onderzoeker bij het Instituut voor Informatierecht.

De Chinese hackersgroep GoldFactory gebruikt zogenoemde malware om de gezichten uit iOS- en Androidapparaten te halen. Malware bestaat uit apps die niet uit de officiële Play Store of App Store komen en als doel hebben om gegevens van apparaten te stelen.

Gezichtsscan

Via phishing installeren dat soort kwaadaardige programma's zich ongewild en vaak ongemerkt op telefoons. De hackers hebben vervolgens toegang tot de gegevens op dat apparaat, zoals inloggegevens, de vingerafdruk en gezichtsscan die mensen gebruiken om hun telefoon en apps te ontgrendelen.

Als criminelen die data eenmaal in handen hebben, kunnen ze met behulp van kunstmatige intelligentie relatief eenvoudig nepbeelden maken van iemands gezicht, zogeheten deepfakes. Die beelden gebruiken ze om gezichtsscans om de tuin te leiden en zo toegang te krijgen tot bijvoorbeeld je bankrekening, waarna het een koud kunstje is om die leeg te roven.

Het is een nieuwe manier van hacken die zelfs experts verbaast en aangeeft hoe snel de ontwikkeling van kunstmatige intelligentie (oftewel AI) en deepfake wordt misbruikt door criminelen.

„Ik heb dit nog niet eerder gezien, maar het was te verwachten", zegt advocaat en onderzoeker Ot van Daalen, van het Instituut voor Informatierecht.

„De technologie om gezichten te kopiëren en dus daarmee deepfakes te maken, ontwikkelt zich steeds verder. Banken maken nog steeds gebruik van gezichtsherkenning als manier om mensen te identificeren. Voor criminelen wordt het steeds aantrekkelijker om zo bankrekeningen te plunderen."

Gezicht is niet meer van jou

De Chinese hackers gaan momenteel doelgericht op zoek naar slachtoffers met veel geld op hun rekening, voornamelijk in Azië, aldus techwebsite Techradar. Maar ook bij ons dreigt gevaar. Volgens Van Daalen wordt dit zeker een probleem in Nederland.

Hij vreest dat er uiteindelijk helemaal geen malware op je telefoon voor nodig is, maar dat criminelen ook misbruik kunnen maken van foto's en videobeelden die elders zijn gemaakt.

„Je kunt er niets aan doen. Foto's van jouw gezicht staan overal op het internet, op straat loop je langs camera's en die filmen je. Ook die gegevens zijn te stelen. Het is onmogelijk om dat te omzeilen."

Dat komt mede doordat onze maatschappij is „ingericht op het vertrouwen dat een gezicht van jou is en dat je deze niet kan veranderen, maar dat klopt niet meer. Mensen kunnen jouw gezicht stelen en namaken", aldus Van Daalen.

Extra laag beveiliging niet voldoende

Als ons gezicht nergens meer veilig is voor kwaadwillenden, is het dus niet meer aan de consument en gebruikers van de app om te voorkomen dat de bankrekening wordt geplunderd. Volgens Van Daalen ligt de verantwoordelijkheid van de veiligheid daarom bij de banken en andere bedrijven die gebruikmaken van gezichtsherkenning.

„Banken moeten nu zorgen dat beveiligingsmethodes rekening houden met deze manier van diefstal. Als ze gebruikmaken van gezichtsherkenning, moeten ze zich weren tegen deepfake."

'Klik niet op linkjes'

Bij navraag blijkt dat ING op de hoogte is van het risico van nepbeelden van gezichten. Zelf geeft de bank aan „diverse zichtbare en onzichtbare maatregelen te nemen die ervoor zorgen dat onze klanten veilig kunnen bankieren."

De bank benadrukt dat klanten zelf ook alert kunnen zijn op malware die deze gegevens van hun apparaten kan stelen. „Wij waarschuwen onze klanten ook altijd om niet op linkjes te klikken waardoor je mogelijk malware kan downloaden."

Fraude en diefstal

Net als Van Daalen ziet ING dat de manier waarop criminelen te werk gaan telkens verandert en inventiever wordt. „AI is een belangrijke ontwikkeling die al op grote schaal wordt gebruikt in de wereld om ons heen. We nemen dit soort technologieën zeer serieus en houden de ontwikkelingen hierover in de gaten om te bepalen hoe we hier in onze dienstverlening rekening mee houden."

ING stelt dat criminelen dankzij AI ontzettend veel nieuwe mogelijkheden krijgen om fraude en diefstal te plegen.

Sociale media

Daarmee geeft ING in ieder geval gehoor aan de oproep van Van Daalen. „ING zal, zoals we dat al jaren doen, klanten waarschuwen via onze campagnes over de laatste ontwikkelingen." In de strijd tegen fraude wordt daarnaast samengewerkt met onder andere de politie en de Nederlandse Vereniging van Banken.

Uiteindelijk kunnen consumenten niets doen tegen het stelen van hun gezicht, daarvoor staan beelden daarvan te vaak op Facebook, Instagram of andere sociale media.

Zelf kunnen consumenten wel goed letten op de apps die ze downloaden. Download alleen applicaties uit de App Store en Play Store en nooit applicaties via andere websites. Dat is namelijk dé manier waarop hackers in hun zoektocht naar nieuwe slachtoffers hun kwaadaardige programma's op je telefoon proberen te zetten.

Load-Date: April 7, 2024

End of Document