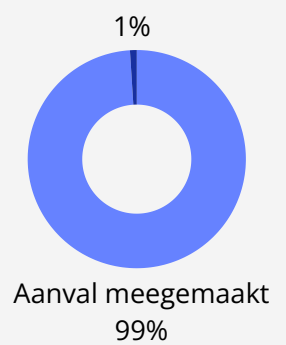


FACTSHEET AI & CYBERCRIME

**AI MAAKT
CYBERCRIMINALITEIT
SNELLER,
GELOOFWAARDIGER &
MAKKELIJKER SCHAALBAAR**

99% van de organisaties wereldwijd maakte het afgelopen jaar minstens één aanval mee op hun AI systemen.



Risico van Grok en deepfakes

Er is kritiek op de AI-chatbot Grok vanwege het genereren van seksuele deepfakes. De Europese Commissie is zelfs een gerechtelijke procedure gestart om een verbod op de chatbot in de EU af te dwingen, omdat xAI, het bedrijf achter Grok, volgens hen onvoldoende maatregelen neemt om de zogenaamde uitkleedfunctie te beperken. De gevolgen zijn aanzienlijk; deepfakes kunnen worden gebruikt voor chantage, online pesten en online seksueel misbruik.

Hoe gebruiken criminelen AI?

Slimmere phishing & oplichting

Criminelen gebruiken AI om phishing en oplichting overtuigender te maken. Berichten zijn foutloos, professioneel en vaak persoonlijk door gebruik van data uit sociale media en datalekken → Hierdoor is fraude moeilijker te herkennen.

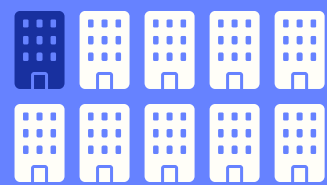
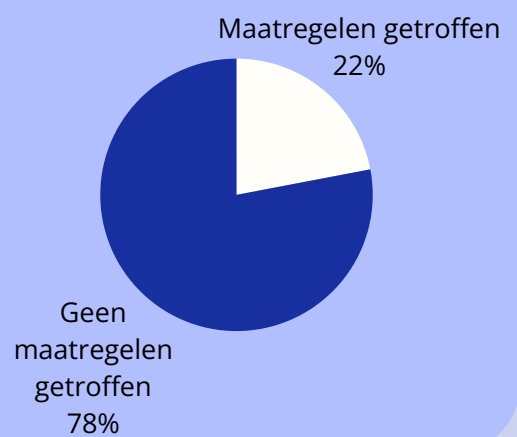
Chatbots & LLM's

AI wordt ingezet om fraude te automatiseren. Phishingmails, scamscripts en gesprekken worden automatisch gegenereerd → Dit verlaagt de drempel en vergroot de schaal van cybercriminaliteit.

Deepfakes (beeld & stem)

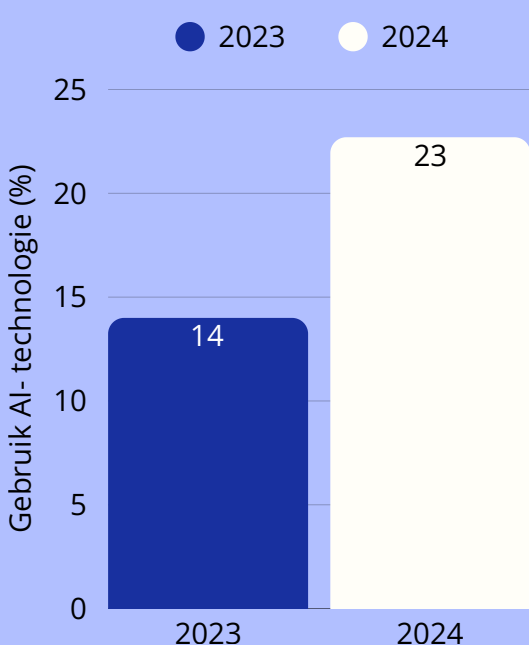
AI kan gezichten en stemmen realistisch namaken. Dit wordt gebruikt voor neptelefoontjes, nepvideo's en CEO-fraude.

Maar 22% van de organisaties is voorbereid op AI-gestuurde identiteitsfraude.



'Minder dan 1 op de 10 antifraudeprofessionals voelt zich goed voorbereid op AI-fraude.'

Gebruik van AI-technologieën door bedrijven



Deepfakes zijn 6,5% van alle fraudecases

Dat is een grote stijging ten opzichte van drie jaar geleden.



Deepfake-fraude: twee soorten aanvallen

- Presentatie-aanvallen:** misleiden van systemen met gemanipuleerde beelden.
- Injectieaanvallen:** voegen misleidende of schadelijke invoer toe om een systeem ongewenst te laten handelen.

Bronnen

- AI maakt fraude slimmer dan ooit - Rockingrobots
- Grok en deepfakes | Digiwijzer
- 2025 Cloud Security Research Report - Palo Alto Networks
- Gebruik kunstmatige intelligentie (AI) door bedrijven neemt toe | CBS
- Europese Commissie wil verbod op AI-chatbot Grok afdwingen via rechter | Tech | NU.nl
- Hacking op basis van AI: soorten AI-cybercriminaliteit en hoe u veilig blijft
- Artificial intelligence, authentic risk: AI-powered threats to soar, warn anti-fraud professionals | SAS