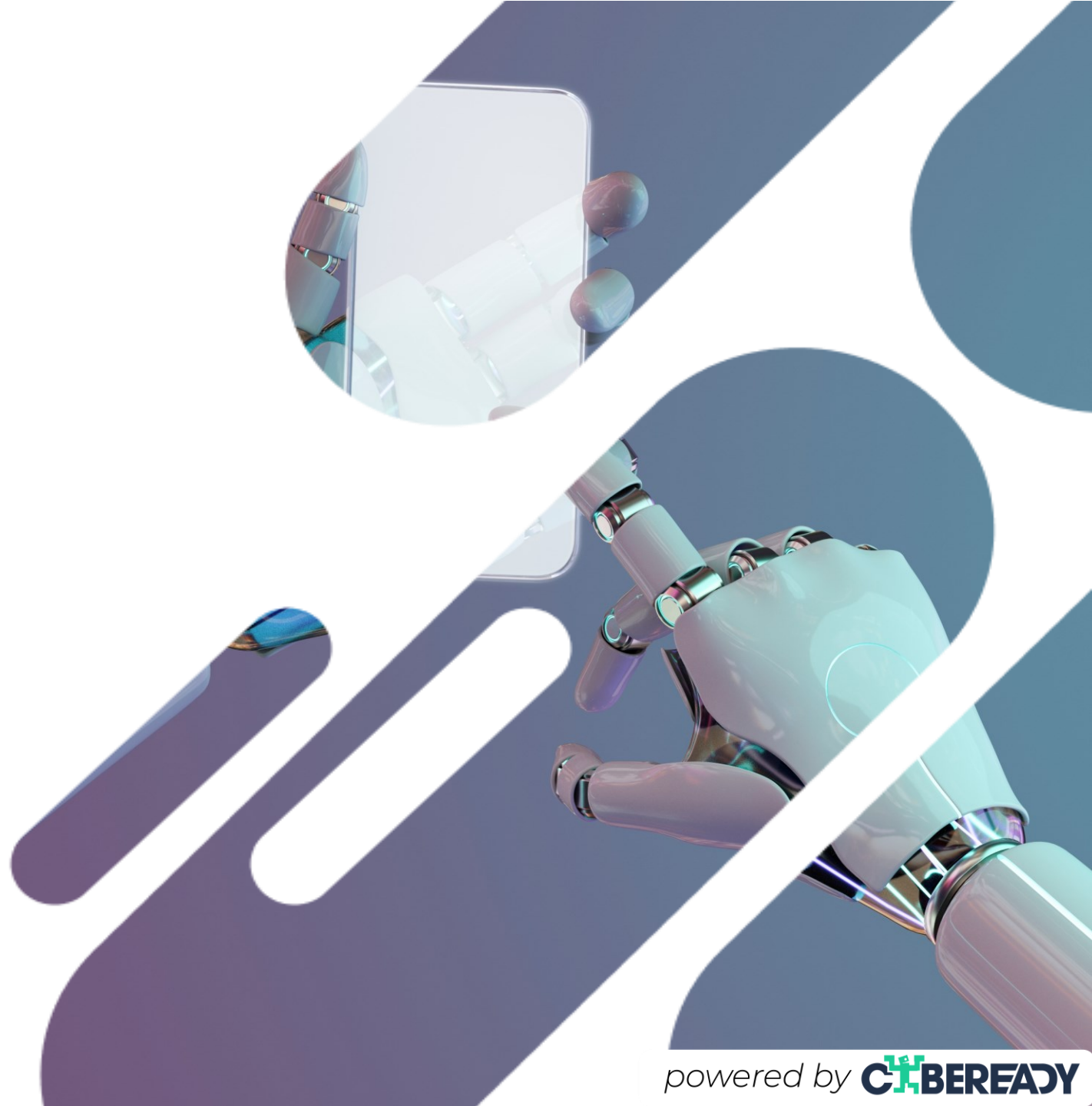




**AI geeft hackers
nieuwe kansen.**

**Bent u erop
voorbereid?**



powered by **CYBERREADY**

Vroeger ...

... kostte het opzetten van heel gesofisticeerde aanvallen veel tijd en werk. Alleen ervaren hackers waren ertoe in staat.

Daardoor **waren de meeste phishingpogingen amateuristisch level** (bv. met spelfouten, een verdachte vormgeving, een fout taalgebruik enz.), zodat wij ze vrij gemakkelijk konden herkennen.





Nu ...

... helpen AI tools de hackers om snel en gemakkelijk e-mails aan te maken met een heel professionele aanblik en inhoud.

Daardoor **krijgen we nu meer gesofisticeerde aanvallen in onze mailbox.** Deze heel bedrieglijke aanvallen zijn moeilijker als dreigingen te identificeren. Het risico dat we in de val trappen, neemt dus toe.

Hoe kunt u phishing nu herkennen?

- Ga na of het **adres van de afzender** van e-mails exact met het verwachte adres overeenkomt. Dat gegeven kunnen hackers niet vervalsen.
- Houd de muisaanwijzer op **links** voor u klikt, zodat u kunt zien of ze legitiem zijn. Hackers kunnen wel de websites van bekende bedrijven nabootsen, maar kunnen hun echte domein niet gebruiken.



Wat is **niet langer** een betrouwbaar teken van authenticiteit?

- Een professioneel design
- Goed geschreven tekst
- Een stemopname van iemand die u kent
- Video's van goede kwaliteit

Niet vergeten: Onze veiligheid ligt in uw handen.

Maak er een gewoonte van om elke e-mail te controleren voor u op een link klikt. Behandel uw e-mail nooit wanneer u verstrooid bent.

