



De schaduwzij den van AI op het werk



Artificiële intelligentie verhoogt de risico's op het werk

AI-tools kunnen wonderen doen voor de productiviteit, maar houden ook grote **risico's in**.

Deze risico's kunnen gevolgen hebben voor de toekomst van ons bedrijf en ook voor u persoonlijk.

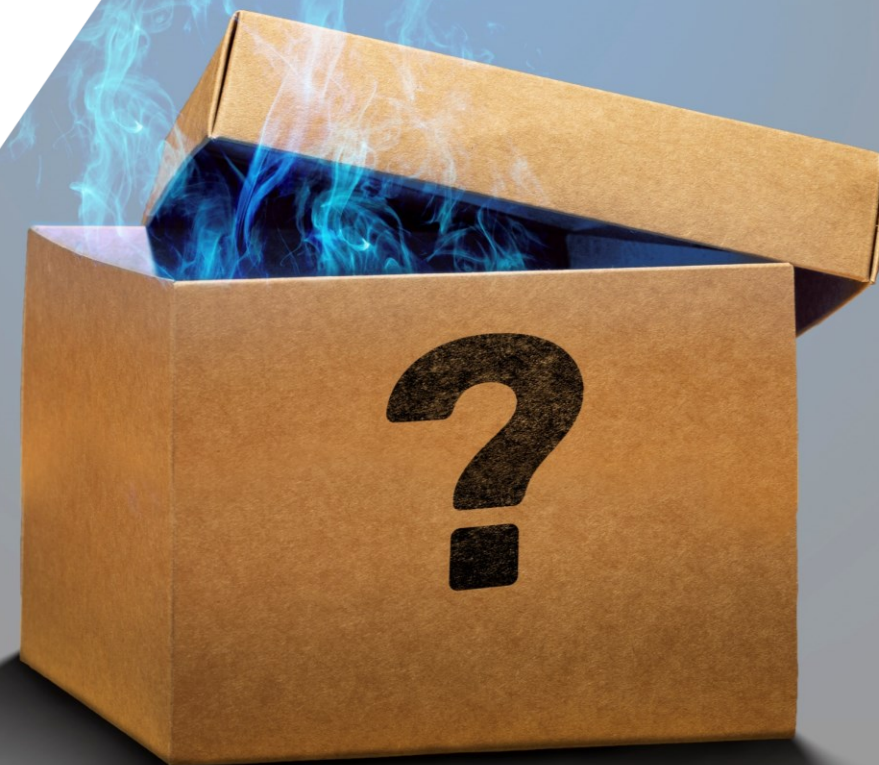
Hoe kan generatieve AI gevaarlijk zijn?

- 1** Vertrouwelijke bedrijfsgegevens onthullen
- 2** Ongeoorloofd gebruik van auteursrechtelijk beschermd materiaal
- 3** Implementatie van foute antwoorden en kwaadwillige code



1 Vertrouwelijke informatie onthullen

Conversaties met AI engines lijken privé, maar **ze verzamelen alles wat we invoeren**: teksten, afbeeldingen, code (dat staat in hun gebruiksvoorwaarden!). We kunnen niet controleren hoe AI onze gegevens gebruikt om modellen te trainen en met anderen te delen, en we kunnen ons er niet tegen beveiligen.



1 Vertrouwelijke informatie onthullen

Wat kunt u doen?



Gebruik geen persoonsgegevens (namen, e-mailadressen enz.) in uw opdrachten voor AI-engines.



Verwijder financiële informatie, broncode of interne mededelingen uit uw opdrachten.



Voer geen inhoud die verband houdt met de bedrijfsstrategie in AI engines in.

2 Auteursrechtelijk beschermde inhoud gebruiken

AI engines verzamelen gegevens, waaronder bedrijfseigen informatie. Een ongeregeld gebruik van de gegevens kan ernstige problemen veroorzaken—zoals **een onopzettelijk gebruik van AI-resultaten die inbreuk maken op auteursrechtelijk beschermd materiaal**. Dat kan ernstige juridische gevolgen hebben voor bedrijven en gebruikers.



2 Auteursrechtelijk beschermde inhoud gebruiken

Wat kunt u doen?



Wijzig door AI gegenereerde teksten of afbeeldingen om een eindproduct te creëren dat van u is.



Wanneer u door AI gegenereerde antwoorden woordelijk gebruikt, moet u hun bron vermelden.



Noem in uw opdrachten geen specifieke artiesten, entiteiten of werken.



Creëer unieke, specifieke opdrachten, om de kans te verkleinen dat AI een creatie van iemand anders genereert.

3 Implementatie van valse informatie en kwaadwillige code

AI engines leveren niet altijd betrouwbare informatie. **De implementatie van fouten of schadelijke code** in uw werk kan ernstige problemen veroorzaken met hackers, klanten en juridische gevolgen.



3 Implementatie van fouten en kwaadwillige code

Wat kunt u doen?



Controleer alle informatie en code uit AI-bronnen. Als u de geldigheid niet kunt verifiëren, vraagt u het aan een expert.



Test met AI gegenereerde code grondig voor u ze implementeert.

Welke soorten AI zijn gevaarlijk?

Alle bestaande engines en platformen.

De populariteit van een engine of het type geproduceerde media maakt geen verschil, de problemen die we hebben aangestipt zijn in alle gevallen identiek.

Wanneer we generatieve AI gebruiken, moeten we altijd maatregelen nemen om ons te beschermen.



A large, glowing speech bubble on the left side of the slide. The bubble's outline is a vibrant blue, while its interior is a deep purple. Three glowing circles, colored in a gradient from pink to blue, are arranged horizontally in the center of the bubble, resembling eyes or a digital face. The background of the slide is a dark blue gradient with a diagonal split.

Niet vergeten:

Generatieve AI is een complexe nieuwe wereld.

Hebt u vragen, wenst u advies of wilt u iets melden?

Aarzel niet om **contact met ons op te nemen.**