



Temná stránka AI v práci





Umělá intelligence zvyšuje rizika na pracovišti

Nástroje umělé intelligence sice mohou zvýšit vaši produktivitu na nevídanou úroveň, ale současně přinášejí velká **rizika**.

Tato rizika mohou ovlivnit budoucnost naší společnosti i vaši budoucnost.

Jak může být generativní AI nebezpečná?

1 Odhalení utajovaných firemních dat

2 Neoprávněné používání materiálů chráněných autorskými právy

3 Implementace nesprávných odpovědí a škodlivého kódu



1 Odhalení důvěrných informací

Konverzace s enginy AI se může jevit jako soukromá, ale **sbírají vše, co zadáme**: text, obrázky, kód (Mají to v podmínkách používání!). Nemáme žádnou kontrolu ani ochranu nad tím, jak AI používá naše data k trénování svých modelů a jak je sdílí s ostatními.



1 Odhalení důvěrných informací

Co můžete dělat?



V dotazech na enginy AI neuvádějte osobní údaje (například jména, e-mailové adresy atd.).



Z dotazů odstraňte finanční údaje, zdrojový kód i veškerou interní komunikaci.



Nevkládejte do enginů AI jakýkoli obsah související se strategií společnosti.

2 Používání obsahu chráněného autorskými právy

Enginy AI shromažďují data, včetně informací chráněných autorským právem. Takové neregulované používání může vést k velkým problémům – například k

neúmyslnému používání výstupů AI, které porušují chráněný materiál. Společnosti a uživatelé by v

důsledku toho mohli nakonec nést závažné právní důsledky.



2 Používání obsahu chráněného autorským právem

Co můžete dělat?



Textové výsledky nebo obrázky z enginu AI upravte a vytvořte konečný produkt, který bude váš.



Pokud používáte odpovědi generované AI doslova, uveďte transparentně zdroj.



V dotazech se vyhněte uvádění konkrétních umělců, subjektů nebo děl.



Vytvářejte jedinečné, specifické výzvy, abyste snížili pravděpodobnost, že AI vygeneruje výtvar někoho jiného.

3 Implementace falešných informací a škodlivého kódu

Enginy AI nemusí vždy poskytovat spolehlivé informace. **Implementace chybného nebo škodlivého kódu** ve vaší práci může způsobit vážné problémy s hackery, pro zákazníky a může to mít právní dohru.



3 Implementace chyb a škodlivého kódu

Co můžete dělat?



Všechny informace i kód z enginů UI dobře zkontrolujte. Pokud nejste schopni platnost, obraťte se na odborníka.



Kód vygenerovaný AI důkladně otestujte, než ho použijete.

Jaké druhy AI jsou rizikové?

Všechny stávající enginy a platformy.

Nezáleží na tom, jestli je engine populární ani na tom, jaký typ médií je vytvářen. Problémy, o kterých jsme hovořili, se vztahují na všechny.

Kdykoli používáme generativní UI, musíme přijmout opatření a chránit se.



A large, stylized speech bubble on the left side of the slide. It has a glowing outline that transitions from pink on the left to blue on the right. Inside the bubble are three small, glowing circles in the same pink-to-blue gradient. The background of the slide is dark blue with a diagonal split.

Nezapomínejte:

Generativní AI představuje komplexní, dosud neprobádaný svět.

Máte otázky, potřebujete poradit nebo chcete něco nahlásit?
Neváhejte nás **kontaktovat**.