

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **136** ze dne **10.3.2026**

Je ChatGPT bezpečný? Jak AI chatbota používat správně

ChatGPT od firmy OpenAI je chatbot využívající velký jazykový model (LLM), což je systém trénovaný na velkém množství textu a kódu schopný analyticky předvídat budoucí vývoj. Funguje tak, že rozpoznává statistické vzorce v jazyce a na jejich základě generuje slova a věty, která budou s největší pravděpodobností následovat.

Konverzace, které s ChatGPT vedeme, se nezpracovávají lokálně, ale na serverech OpenAI, kde (v bezplatné verzi / ChatGPT Plus) taky zůstávají uloženy, dokud nepožádáme o jejich vymazání. A to je možné jen v případě registrovaných uživatelů. Dobře si rozmyslet, jaké informace chatbotovi svěříme, je tedy pro ochranu našich dat naprosto zásadní.

Jak ChatGPT chrání svoje uživatele?

Co se týče šifrování komunikace, ChatGPT využívá stejných standardů jako třeba banky. Při přihlašování umožňuje vícefázové ověření a podléhá obecnému nařízení o ochraně osobních údajů (GDPR). Kromě toho provádí i základní moderaci obsahu.

I přesto je ale používání AI chatbotů spojené s určitými bezpečnostními riziky, kterými jsou například:

Úniky dat a krádeže přihlašovacích údajů

Už v březnu 2023 si uživatelé ChatGPT začali všimnout, že se jim v historii objevují cizí zprávy. Chyba byla na straně OpenAI a vznikla zranitelnost v systému. Rok nato se na dark webu objevilo přes 100 tisíc ukradených přihlašovacích údajů, které pocházely hlavně ze zařízení oslabených malwarem, který mohl (ale nemusel) vzejít z podvodné aplikace.

Falešné aplikace a phishing

Obchody aplikací a rozšíření do prohlížečů nabízejí falešné aplikace, které jsou od skutečného ChatGPT na první pohled k nerozeznání, ale slouží jen ke sběru přihlašovacích údajů a/nebo instalaci malware. Při stahování ChatGPT aplikací je vždy nutné ověřit si, že jejím autorem je OpenAI.

Trénování modelů a ochrana soukromí

Všechno, co v bezplatné verzi nebo ChatGPT Plus do konverzace napíšeme, využívá OpenAI k dalšímu trénování svých modelů. Data jsou sice anonymizovaná, ale v kontextu můžou i tak odhalit citlivé informace. Autorizovaní zaměstnanci OpenAI mají navíc z bezpečnostních důvodů do některých chatů přístup.

Chybné informace a halucinace

ChatGPT někdy sebevědomě předkládá úplně smyšlené informace, kterým se říká halucinace. Ke všem odpovědím proto přistupujte jako k neověřeným informacím, dokud si je nepotvrdíte v důvěryhodných zdrojích.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **136** ze dne **10.3.2026**

Malware a sociální inženýrství

Internetoví útočníci si pomocí umělé inteligence generují malware, vzorové phishingové zprávy nebo přesvědčivé deepfaky, což jim značně usnadňuje provádění kybernetických útoků. Zároveň to dramaticky navyšuje počet útočníků, protože už nepotřebují prakticky žádnou specializaci.

Co s chatbotem nikdy nesdílet?

Už ze samé podstaty služby vyplývá, že zamyslet se nad tím, co a proč s chatbotem sdílíme, bude klíčem k jeho bezpečnému používání. OpenAI sice s nasbíranými daty neobchoduje, ale v zájmu vylepšování služeb je může sdílet se svými dodavateli (např. platebními bránami).

Je tedy v našem zájmu ke každému chatu přistupovat jako k veřejné nástěnce a nikdy nesdílet:

- Osobní údaje jako rodné číslo, čísla dokladů, poštovní adresy apod.
- Finanční informace jako čísla platebních karet, bankovních účtů apod.
- Přihlašovací údaje a kontaktní informace
- Informace o zdravotním stavu
- Firemní data, tzn. jakákoliv data, která podle interních směrnic zaměstnavatele nepatří na veřejnost

Zvlášť opatrní by při používání chatbota měli být lékaři, právní zástupci, finanční poradci a další profese, které denně nakládají s citlivými osobními údaji svých pacientů a klientů. Sdílení takových informací s chatbotem by mohlo znamenat porušení lékařského tajemství, povinnosti mlčenlivosti advokáta nebo GDPR.

Jak ChatGPT používat bezpečně?

ChatGPT je hlavně a přednostně online služba a platí pro ni stejné zásady bezpečnosti jako pro každou jinou. Pokud máte účet, nastavte si silné heslo a vícefázové ověření, které pomůžou ochránit obecnou bezpečnost vašeho účtu.

Pro ochranu soukromí dodržujte následující kroky:

1. Používejte jen oficiální platformu ChatGPT nebo ověřenou aplikaci z Google Play / App Store.
2. Vypněte trénování na svém obsahu v portálu pro ochranu soukromí.
3. Používejte dočasné chaty, na kterých se model netrénuje, zvlášť pro citlivá data.
4. V konverzaci používejte anonymní příklady místo skutečných informací a nikdy do chatu nenahrávejte skutečné dokumenty.
5. Mažte historii a hlídejte si, kde všude jste přihlášení, ať se vám do účtu nedostane někdo nepovolaný.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **136** ze dne **10.3.2026**

-
6. Používejte komplexní bezpečnostní řešení s VPN, které se postará o bezpečnost vašich zařízení i při používání AI chatbotů.

Tak tedy – je ChatGPT bezpečný?

Odpověď je ano i ne. I když využijeme všech dostupných opatření, které OpenAI do svých produktů zahrnula, jejich obchodní model pořád stojí na sběru dat. Pokud k ChatGPT přistupujeme zodpovědně, může nám sloužit dobře a poměrně bezpečně. Svoje data si ale musíme ohlídat sami.

AV centrum ČR