

人工智能(AI)聊天機械人 挑戰與良好使用習慣

什麼是AI聊天機械人？

AI聊天機械人是一種電腦程式，利用AI技術和自然語言處理來理解用戶輸入的語音或文本指示，並像真人般回應用戶。AI聊天機械人可於客戶服務、虛擬助理和電子商貿等各領域，提高營運效率和提供嶄新服務。



挑戰

私隱問題



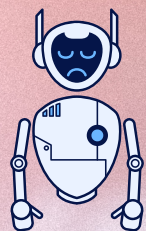
AI聊天機械人用戶未必完全了解其個人資料如何被收集、儲存或保留，或是否會未經授權或意外地被查閱、處理、刪除、喪失或使用。與其他資訊系統或應用程式一樣，AI聊天機械人有機會受到網絡攻擊，因而導致數據外泄。

偏見



AI聊天機械人的回應可能會出現偏見。如數據集內容有欠多元化、供訓練用的數據集內容不準確，或源自數據的偏見，都會增加產生帶有偏見或歧視成分的答案的可能性。

錯誤和不準確的資訊



同樣地，不足或過時的訓練數據亦會影響AI聊天機械人的準確性。有時，AI聊天機械人可能為了產生流暢的反應而編造內容，導致資訊不準確。此外，AI聊天機械人也可能會誤解用戶的原意或意思，因而提供不正確的資訊。

侵犯知識產權



AI聊天機械人可能會在未經授權下使用了受版權保護的素材或專有資訊，可能導致侵犯知識產權。

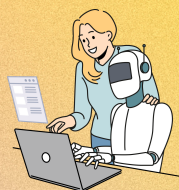
濫用



AI聊天機械人有機會被惡意濫用，例如用作開發惡意軟件，或製造更具說服力和個性化的社交工程攻擊。

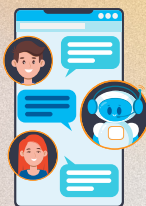
良好作業模式

使用AI聊天機械人作為輔助工具



AI聊天機械人可以有助收集資訊和提供基本支援，但不應純粹依賴它們，應從其他來源核實資訊。

負責任地使用AI聊天機械人



合法並合乎道德地使用AI聊天機械人。不要向AI聊天機械人提出超越其功能所限的要求，或將其用於惡意用途。

緊記AI聊天機械人並非完美



要注意AI聊天機械人可能會提供片面或不準確的資訊。

如果AI聊天機械人產生帶有偏見或歧視成分的回應，應向其供應商報告。

保護私隱和數據



避免向AI聊天機械人輸入敏感或個人資料。

選用信譽良好和素以講求數據安全著稱的公司所提供的AI聊天機械人。

