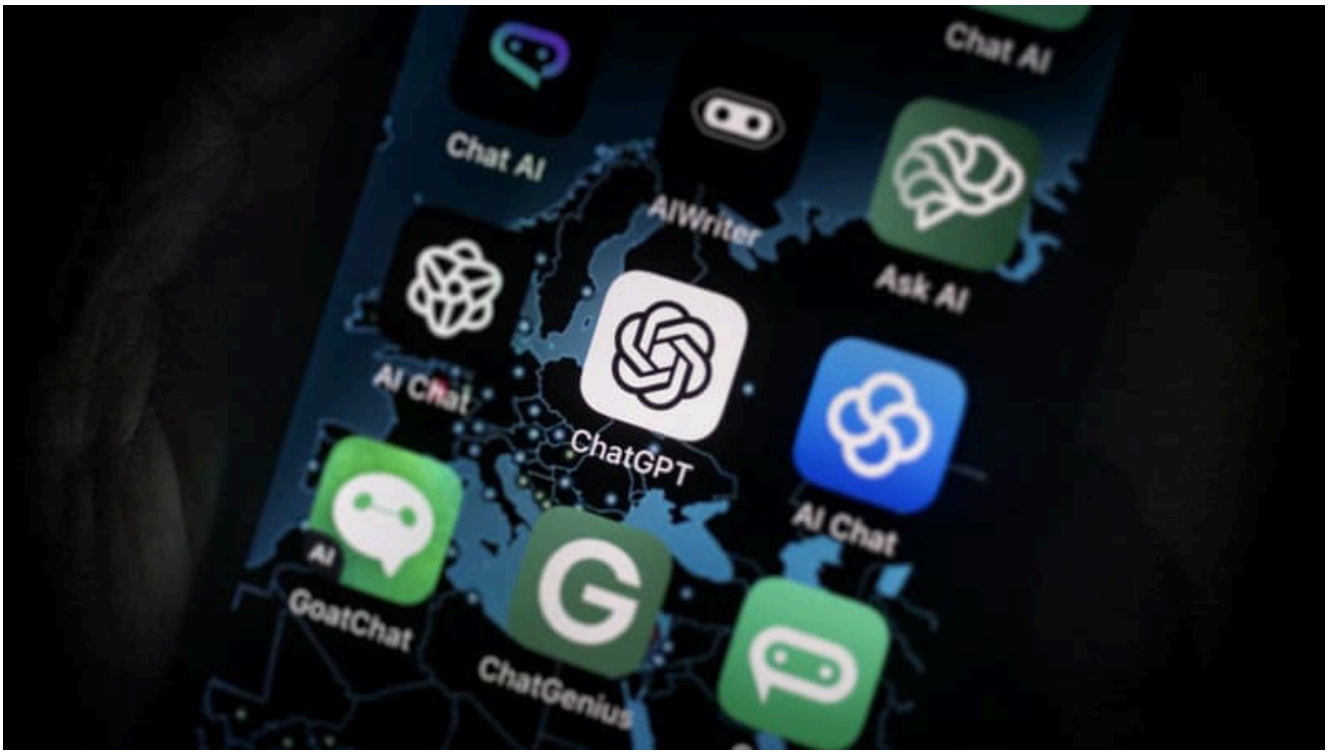
Les pièges de la confiance : pourquoi se méfier de ChatGPT

ChatGPT : Deux Ans D’Intelligence Artificielle



Le 30 novembre 2024, ChatGPT célèbre un tournant dans son histoire. En l’espace de deux années, cette création d’OpenAI s’est imposée comme bien plus qu’un simple assistant virtuel. Mais il est crucial de savoir qu’il y a des limites à ce que l’on peut lui confier.

Depuis son lancement en novembre 2022, ChatGPT a connu des avancées notables. L’intelligence artificielle, initialement conçue pour répondre à des questions par écrit, a fait un bond en avant significatif. En effet, depuis septembre 2023, le chatbot est capable de converser oralement. Tout récemment, OpenAI a également introduit un mode vocal avancé qui rend les

interactions plus humaines et naturelles.

Avec cette nouvelle fonctionnalité, les utilisateurs peuvent désormais interrompre le chatbot, et ce dernier peut s'exprimer avec un éventail d'émotions, ce qui modifie la nature de l'échange.

Un Compagnon et un Écouteur

Cette capacité de conversation a amené de nombreux utilisateurs à partager des réflexions personnelles avec ChatGPT. Un utilisateur a notamment déclaré sur X (anciennement Twitter) : *"J'aime utiliser le mode vocal en conduisant, c'est devenu mon moyen de communication préféré."* D'autres utilisateurs partagent des expériences similaires, révélant que cette IA deviendrait même, pour certains, un ami ou un confident.

Cependant, confier ses pensées les plus intimes à une intelligence artificielle soulève des questions de sécurité. Bien que ChatGPT assure que les interactions restent confidentielles, il recommande aux utilisateurs de rester prudents avec des détails sensibles qui pourraient causer des problèmes futurs.

Les Risques de Fuite d'Informations

Des fuites de données ont déjà été signalées, notamment parmi les employés de Samsung, qui ont utilisé ChatGPT pour traiter des informations confidentielles en 2023. Cet incident a conduit certaines entreprises, comme Samsung, à interdire l'utilisation de ce type de technologie au sein de leurs équipes, en raison des conséquences potentielles sur la confidentialité des données.

De plus, des failles de sécurité ont permis la divulgation d'informations personnelles d'utilisateurs, y compris des

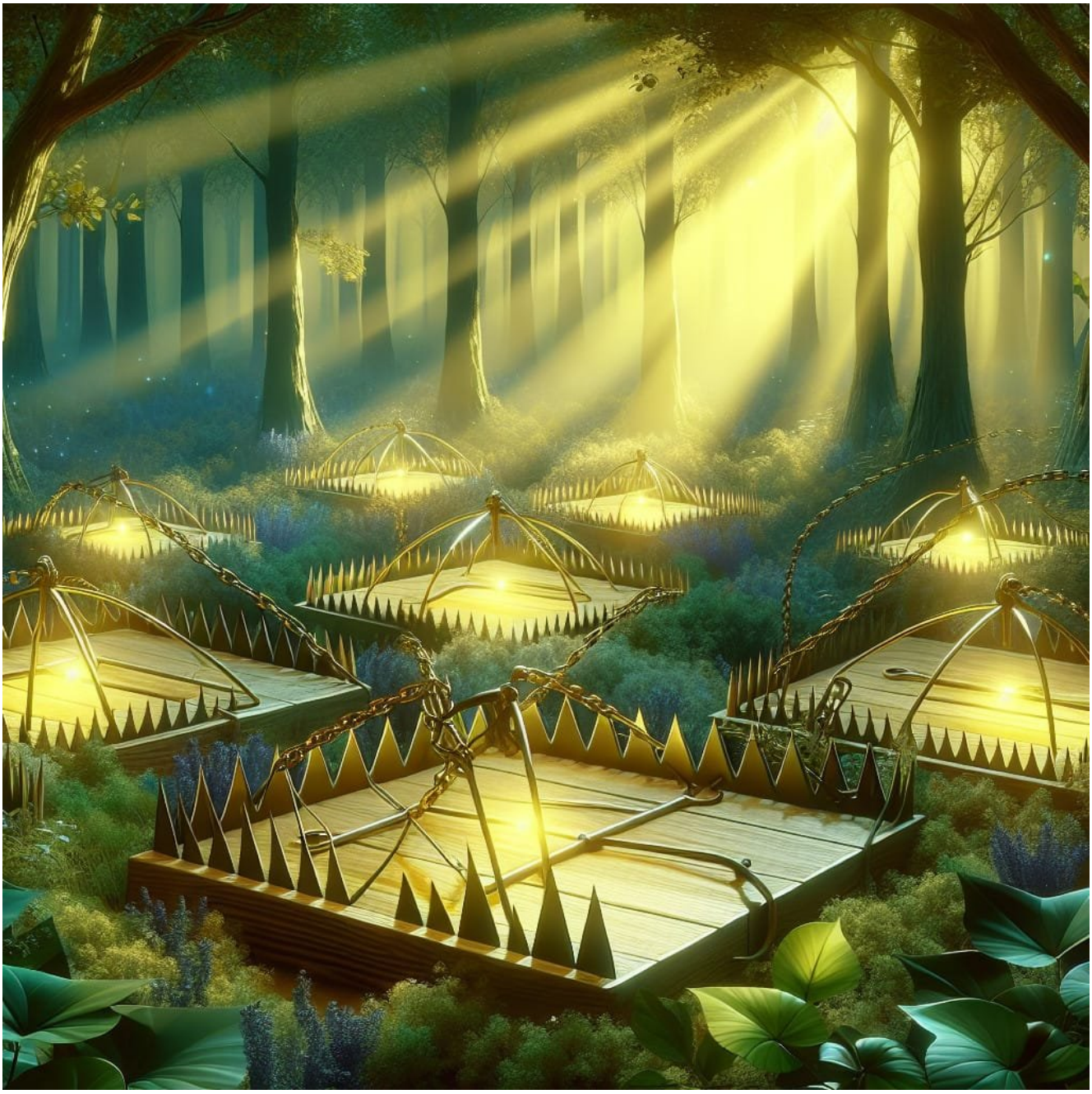
journalistes. Bien que OpenAI ait mis en place des mesures de sécurité, telles que le chiffrement des données, la prudence est de mise.

Améliorations et Mémoire

OpenAI a également introduit des mises à jour concernant la gestion de la mémoire de ChatGPT. Le chatbot peut maintenant mémoriser des informations lors des discussions avec les utilisateurs, afin de mieux les comprendre et d'améliorer le niveau de personnalisation des échanges. Toutefois, cette mémoire est activée par défaut, ce qui signifie qu'il est essentiel pour les utilisateurs de gérer cette fonctionnalité en toute connaissance de cause.

Pour une expérience plus éphémère et sécurisée, les utilisateurs peuvent activer une session de "chat éphémère", où l'IA ne retiendra pas les détails de la conversation. Bien que cela offre une certaine tranquillité d'esprit, OpenAI prévient que des copies des chats peuvent être gardées pour des raisons de sécurité pendant une période maximale de 30 jours.

> *"Pour des raisons de sécurité, nous pouvons conserver une copie pendant 30 jours au maximum," précise OpenAI.*



Au final, il est essentiel d’être conscient des implications de l’utilisation de ChatGPT, surtout lorsqu’il s’agit de partager des informations personnelles. La technologie évolue, et avec elle, les précautions à prendre lors de son utilisation.

Source : www.bfmtv.com

→ Accéder à CHAT GPT en cliquant dessus