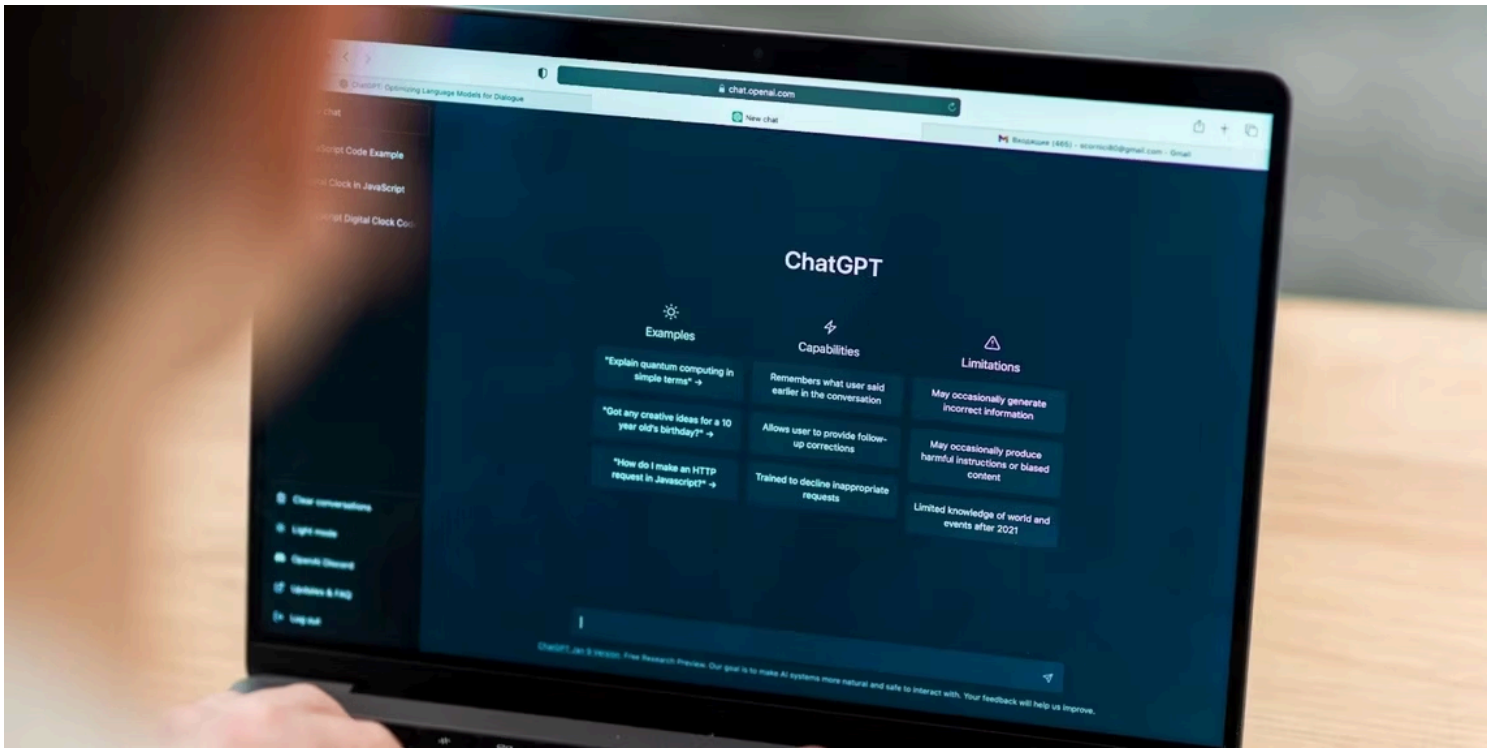
5 choses que vous ne devez pas partager avec les chatbots IA

Les conversations avec les chatbots peuvent sembler intimes, mais vous partagez vraiment chaque mot avec une entreprise privée.

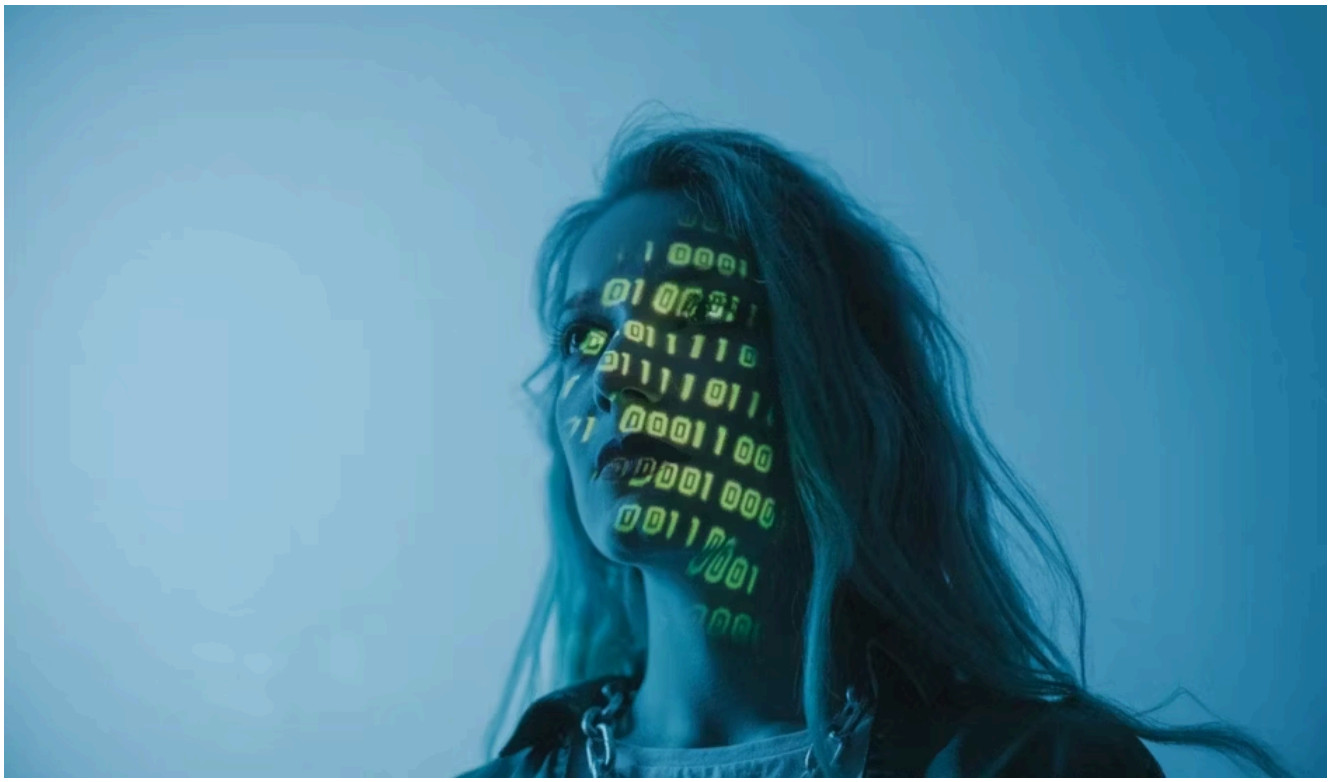
Wasay Ali ⋮



La popularité des chatbots d'intelligence artificielle a explosé.
Bien que leurs capacités soient impressionnantes, il est important de reconnaître que les chatbots ne sont pas sans faille.
Il existe des risques inhérents associés à l'utilisation de chatbots basés sur l'IA, tels que les préoccupations en matière de confidentialité et les cyberattaques potentielles.
Il est crucial de faire preuve de prudence lorsque vous interagissez avec des chatbots.

Explorons les dangers potentiels du partage d'informations avec des chatbots IA et voyons quels types d'informations ne doivent pas leur être divulgués.

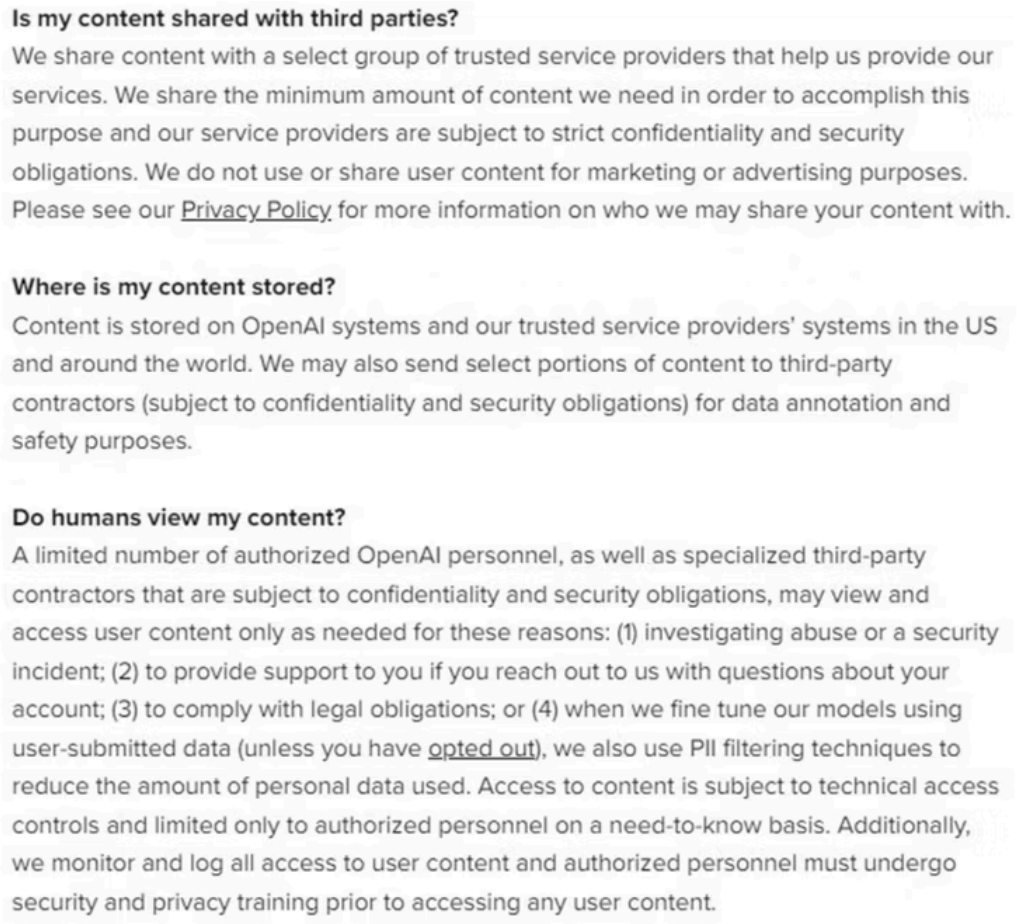
Les risques liés à l'utilisation de chatbots basés sur l'IA



Les risques d'atteinte à la vie privée et les vulnérabilités associés aux chatbots d'IA posent des problèmes de sécurité importants pour les utilisateurs.
Cela peut vous surprendre, mais vos compagnons de chat amicaux comme ChatGPT, Gemini, Copilot et d'autres peuvent exposer par inadvertance vos informations personnelles en ligne.
Ces chatbots s'appuient sur des modèles de langage d'IA, qui tirent des informations de vos données.

Par exemple, la version actuelle du chatbot de Google, Gemini, indique explicitement sur sa page FAQ qu'elle collecte et utilise les données de conversation pour entraîner son modèle.
De même, ChatGPT a également des problèmes de confidentialité car il peut conserver les enregistrements de chat pour améliorer le modèle.
Mais il offre une option pour se désinscrire.

Étant donné que les chatbots IA stockent des données sur des serveurs, ils deviennent vulnérables aux tentatives de piratage.
Ces serveurs contiennent une mine d'informations que les cybercriminels peuvent exploiter de diverses manières.
Ils peuvent infiltrer les serveurs, voler les données et les vendre sur les marchés du dark web.
De plus, les pirates peuvent exploiter ces données pour déchiffrer les mots de passe et obtenir un accès non autorisé à vos appareils.



Is my content shared with third parties?

We share content with a select group of trusted service providers that help us provide our services. We share the minimum amount of content we need in order to accomplish this purpose and our service providers are subject to strict confidentiality and security obligations. We do not use or share user content for marketing or advertising purposes. Please see our Privacy Policy for more information on who we may share your content with.

Where is my content stored?

Content is stored on OpenAI systems and our trusted service providers' systems in the US and around the world. We may also send select portions of content to third-party contractors (subject to confidentiality and security obligations) for data annotation and safety purposes.

Do humans view my content?

A limited number of authorized OpenAI personnel, as well as specialized third-party contractors that are subject to confidentiality and security obligations, may view and access user content only as needed for these reasons: (1) investigating abuse or a security incident; (2) to provide support to you if you reach out to us with questions about your account; (3) to comply with legal obligations; or (4) when we fine tune our models using user-submitted data (unless you have opted out), we also use PII filtering techniques to reduce the amount of personal data used. Access to content is subject to technical access controls and limited only to authorized personnel on a need-to-know basis. Additionally, we monitor and log all access to user content and authorized personnel must undergo security and privacy training prior to accessing any user content.

Crédits image : FAQ OpenAI

De plus, les données générées par vos interactions avec les chatbots IA ne sont pas limitées aux seules entreprises concernées.
Bien qu'ils maintiennent que les données ne sont pas vendues à des fins de publicité ou de marketing, elles sont partagées avec certains tiers pour les besoins de maintenance du système.

OpenAI, l'organisation à l'origine de ChatGPT, reconnaît qu'elle partage des données avec « un groupe restreint de fournisseurs de services de confiance » et que certains « membres du personnel autorisé d'OpenAI » peuvent avoir accès aux données.
Ces pratiques soulèvent d'autres problèmes de sécurité concernant les interactions des chatbots d'IA, car les critiques affirment que les problèmes de sécurité de l'IA générative peuvent s'aggraver.

Par conséquent, la protection des informations personnelles contre les chatbots IA est cruciale pour préserver votre vie privée.

Pour garantir votre confidentialité et votre sécurité, il est essentiel de suivre ces cinq bonnes pratiques lorsque vous interagissez avec des chatbots IA.

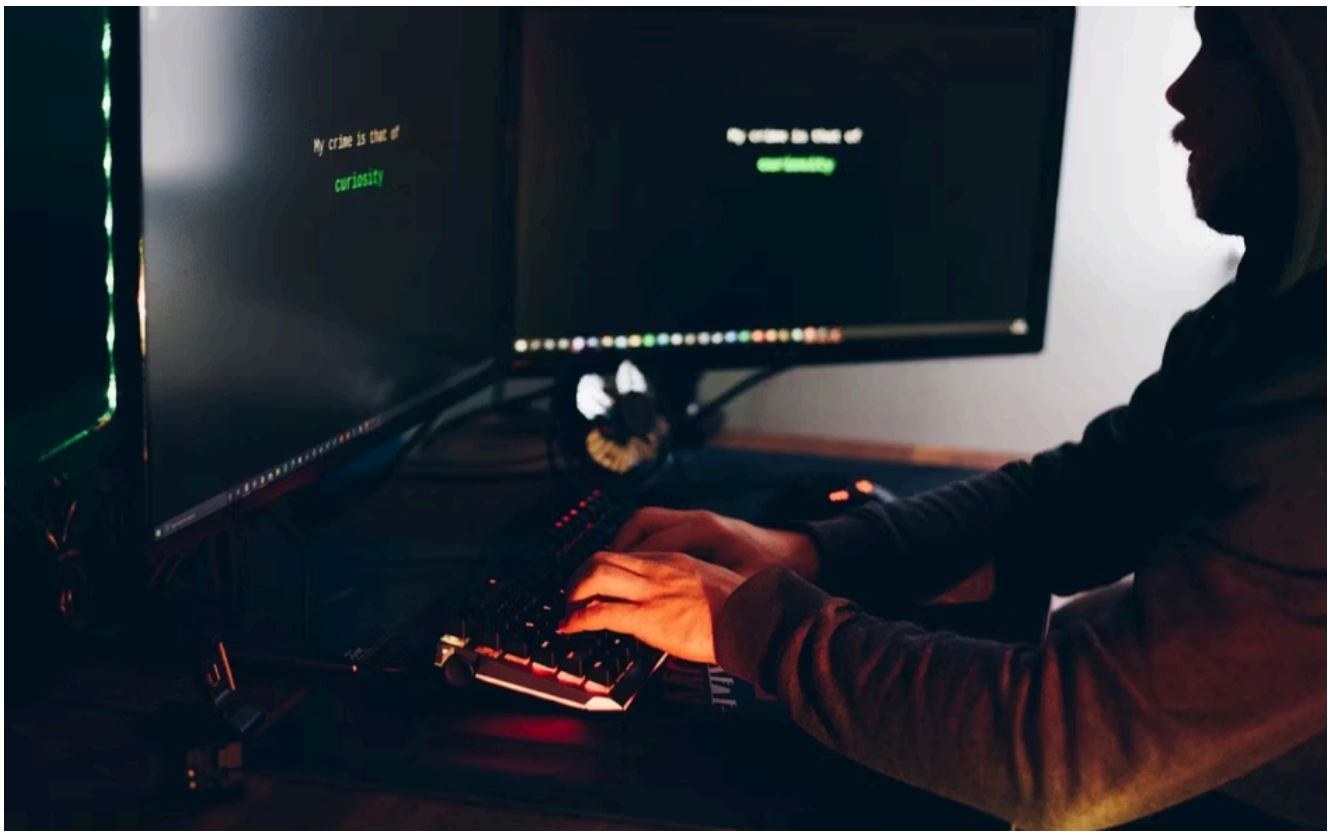
1. Détails financiers

Les cybercriminels peuvent-ils utiliser des chatbots IA comme ChatGPT pour pirater votre compte bancaire ?
Avec l'utilisation généralisée des chatbots d'IA, de nombreux utilisateurs se sont tournés vers ces modèles de langage pour obtenir des conseils financiers et gérer leurs finances personnelles.
Bien qu'ils puissent améliorer la littératie financière, il est essentiel de connaître les dangers potentiels du partage de détails financiers avec des chatbots d'IA.

Lorsque vous utilisez des chatbots comme conseillers financiers, vous risquez d'exposer vos informations financières à des cybercriminels potentiels qui pourraient les exploiter pour vider vos comptes.
Bien que les entreprises prétendent anonymiser les données de conversation, des tiers et certains employés peuvent toujours y avoir accès.
Cela soulève des inquiétudes quant au profilage, où vos informations financières pourraient être utilisées à des fins malveillantes telles que des campagnes de ransomware ou vendues à des agences de marketing.

Pour protéger vos informations financières des chatbots d'IA, vous devez faire attention à ce que vous partagez avec ces modèles d'IA générative.
Il est conseillé de limiter vos interactions à l'obtention d'informations générales et à poser des questions générales.
Si vous avez besoin de conseils financiers personnalisés, il existe peut-être de meilleures options que de vous fier uniquement aux robots d'IA.
Ils peuvent fournir des informations inexactes ou trompeuses, ce qui peut mettre en péril votre argent durement gagné.
Envisagez plutôt de demander conseil à un conseiller financier agréé qui peut vous fournir des conseils fiables et personnalisés.

2. Vos pensées personnelles et intimes



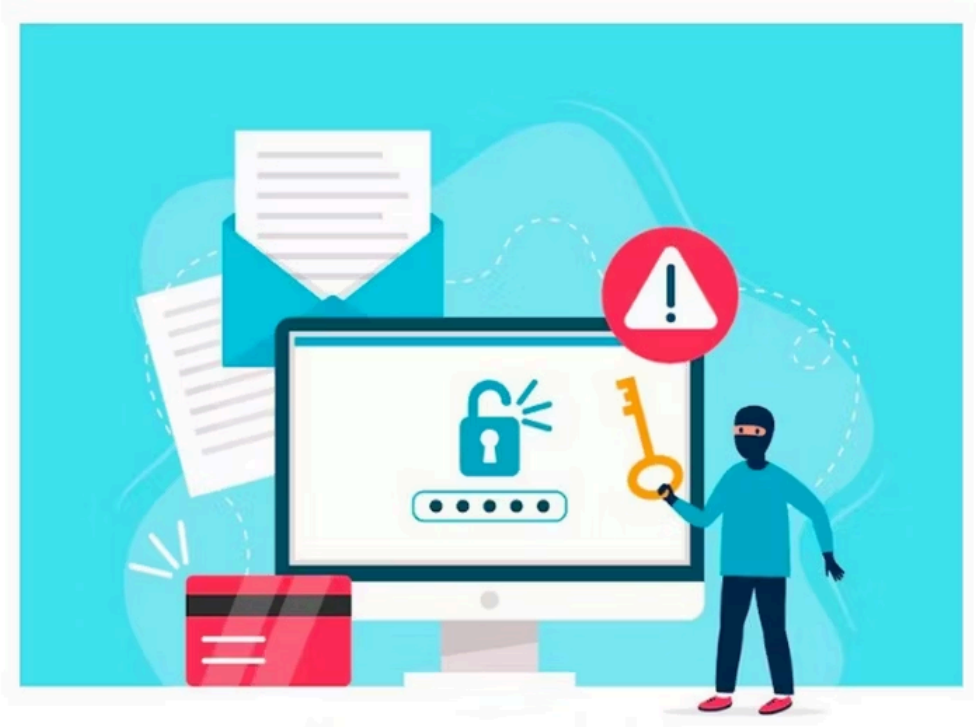
De nombreux utilisateurs se tournent vers les chatbots d'IA pour suivre une thérapie, sans se soucier des conséquences potentielles sur leur bien-être mental.
Il est essentiel de comprendre les dangers de la divulgation d'informations personnelles et intimes à ces chatbots.

Tout d'abord, les chatbots manquent de connaissances du monde réel et ne peuvent offrir que des réponses génériques aux questions liées à la santé mentale.
Cela signifie que les médicaments ou les traitements qu'ils suggèrent peuvent ne pas être adaptés à vos besoins spécifiques et pourraient nuire à votre santé.

De plus, le partage de pensées personnelles avec des chatbots d'IA soulève d'importantes préoccupations en matière de confidentialité.
Votre vie privée peut être compromise car vos secrets et vos pensées intimes peuvent être divulgués en ligne.
Des individus malveillants pourraient exploiter ces informations pour vous espionner ou vendre vos données sur le dark web.
Par conséquent, il est de la plus haute importance de protéger la confidentialité des pensées personnelles lors de l'interaction avec les chatbots IA.

Il est crucial d'aborder les chatbots d'IA comme des outils d'information générale et de soutien plutôt que comme un substitut à une thérapie professionnelle.
Si vous avez besoin de conseils ou d'un traitement en santé mentale, il est toujours conseillé de consulter un professionnel de la santé mentale qualifié.
Ils peuvent fournir des conseils personnalisés et fiables tout en donnant la priorité à votre vie privée et à votre bien-être.

3. Informations confidentielles de votre lieu de travail



Générique de l'image : Freepik

Une autre erreur que les utilisateurs doivent éviter lorsqu'ils interagissent avec des chatbots IA est le partage d'informations confidentielles liées au travail.
Même les géants de la technologie de premier plan tels qu'Apple, Samsung, JPMorgan et Google, le créateur de Gemini, ont interdit à leurs employés d'utiliser des chatbots d'IA sur le lieu de travail.

Un rapport de Bloomberg a mis en évidence un cas où des employés de Samsung ont utilisé ChatGPT à des fins de codage et ont téléchargé par inadvertance du code sensible sur la plate-forme d'IA générative.
Cet incident a entraîné la divulgation non autorisée d'informations confidentielles sur Samsung, ce qui a incité l'entreprise à interdire l'utilisation des chatbots d'IA.
En tant que développeur cherchant l'aide de l'IA pour résoudre les problèmes de codage, c'est la raison pour laquelle vous ne devriez pas faire confiance aux chatbots IA comme ChatGPT pour des informations confidentielles.
Il est essentiel de faire preuve de prudence lorsque vous partagez du code sensible ou des détails liés au travail.

Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

ChatGPT Samsung Data Leak | cybernews.com (youtube.com)

De même, de nombreux employés s'appuient sur des chatbots d'IA pour résumer les procès-verbaux de réunion ou automatiser les tâches répétitives, ce qui présente un risque d'exposition involontaire de données sensibles.
Il est donc de la plus haute importance de préserver la confidentialité des informations professionnelles confidentielles et de s'abstenir de les partager avec des chatbots basés sur l'IA.

Les utilisateurs peuvent protéger leurs informations sensibles et protéger leur organisation contre les fuites ou les violations de données par inadvertance en étant conscients des risques associés au partage de données liées au travail.

4. Mots de passe

Générique de l'image : pch.vector/Freepik

Il est essentiel de souligner que le partage de vos mots de passe en ligne, même avec des modèles de langage, est absolument à proscrire.
Ces modèles stockent vos données sur des serveurs publics, et la divulgation de vos mots de passe met en péril votre vie privée.
Lors d'une violation de serveur, les pirates peuvent accéder à vos mots de passe et les exploiter pour leur causer des dommages financiers.

Une importante violation de données impliquant ChatGPT s'est produite en mai 2022, soulevant de sérieuses inquiétudes quant à la sécurité des plateformes de chatbots.
De plus, ChatGPT a été interdit en Italie en raison du règlement général sur la protection des données (RGPD) de l'Union européenne.
Les régulateurs italiens ont jugé que le chatbot IA n'était pas conforme aux lois sur la protection de la vie privée, soulignant les risques de violations de données sur la plateforme.
Par conséquent, il devient primordial de protéger vos identifiants de connexion contre les chatbots IA.

En vous abstenant de partager vos mots de passe avec ces modèles de chatbots, vous pouvez protéger vos informations personnelles de manière proactive et réduire la probabilité d'être victime de cybermenaces.

N’oubliez pas que la protection de vos identifiants de connexion est une étape essentielle au maintien de votre confidentialité et de votre sécurité en ligne.

5. Données résidentielles et autres données personnelles

Il est important de s’abstenir de partager des informations d’identification personnelle (PII) avec des chatbots d’IA.
Les informations personnelles englobent les données sensibles qui peuvent être utilisées pour vous identifier ou vous localiser, notamment votre emplacement, votre numéro de sécurité sociale, votre date de naissance et vos informations de santé.
Assurer la confidentialité des données personnelles et résidentielles lors de l’interaction avec les chatbots IA devrait être une priorité absolue.

Pour préserver la confidentialité de vos données personnelles lorsque vous interagissez avec des chatbots basés sur l’IA, voici quelques pratiques clés à suivre :

- Familiarisez-vous avec les politiques de confidentialité des chatbots pour comprendre les risques associés.
- Évitez de poser des questions qui pourraient révéler par inadvertance votre identité ou vos renseignements personnels.
- Faites preuve de prudence et évitez de partager vos informations médicales avec des robots d’IA.
- Soyez conscient des vulnérabilités potentielles de vos données lorsque vous utilisez des chatbots d’IA sur des plateformes sociales comme SnapChat.

Évitez de trop partager avec les chatbots IA

En conclusion, bien que la technologie des chatbots IA offre des avancées significatives, elle présente également de graves risques pour la vie privée.
La protection de vos données en contrôlant les informations partagées est cruciale lorsque vous interagissez avec des chatbots d’IA.
Restez vigilant et respectez les meilleures pratiques pour atténuer les risques potentiels et assurer la confidentialité.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240227
"C'est ensemble qu'on avance"