CHATGPT EST-IL FIABLE ET SECURISE ?

ChatGPT a révolutionné la manière dont nous interagissons avec l'IA. Mais, son adoption massive soulève des questions cruciales liées à la sécurité et à la confidentialité des données. **Allan Camps, Senior Enterprise Account Executive chez Keeper Security**, nous livre son point de vue.

ChatGPT est un logiciel d'intelligence artificielle souvent utilisé pour simplifier des sujets complexes, générer des idées, créer des textes semblables à ceux d'un être humain et élaborer du contenu marketing. Selon l'usage que nous en faisons, il peut être un outil fiable et sécurisé. Toutefois, pour vous protéger et protéger vos données, vous devez être conscient de certains risques de sécurité. Ces risques comprennent des inquiétudes concernant la confidentialité, le partage de données avec des sources tierces, des sites web et des applications ChatGPT copiés et la tendance de l'outil à générer des informations erronées.

Les risques de sécurité associés à l'utilisation de ChatGPT

La protection de la vie privée : L'un des plus grands risques de sécurité auxquels vous pouvez être confronté lorsque vous utilisez ChatGPT est la violation de la vie privée. OpenAI, propriétaire de ChatGPT, indique dans sa politique de confidentialité que, dans certaines circonstances, ChatGPT fournira des données d'utilisateur à des tiers sans en informer l'utilisateur. Les informations que vous donnez à ChatGPT lorsque vous utilisez le logiciel sont enregistrées et stockées, et peuvent ensuite être partagées avec des sources tierces.

Les sites web et applications illégitimes : De nombreux escrocs ont commencé à créer des sites Web usurpant l'identité de ChatGPT afin de voler les informations privées des individus. Google Play, la boutique d'applications de Google, a trouvé des centaines d'applications ChatGPT illégitimes en avril 2023, et des millions de personnes ont téléchargé ces fausses applications et révélé leurs données privées à des cybercriminels. Veillez à utiliser le site web et l'application officiels de ChatGPT pour éviter que vos informations ne soient involontairement partagées avec des cybercriminels par le biais de faux sites web et de fausses applications.

Les fausses informations (fakenews) : Bien que ChatGPT puisse produire un contenu écrit semblable à celui d'un humain, cela ne signifie pas toujours que ses réponses sont exactes. ChatGPT est connu pour avoir un comportement de chatbot : ils peuvent spontanément commencer à inventer des informations. Il est donc dangereux de se fier entièrement à ChatGPT pour obtenir des informations exactes tant il est capable de produire des informations erronées comme. Par conséquent, n'utilisez pas ChatGPT comme un outil de recherche, car son contenu ne sera pas toujours vrai ou exact. Tout contenu créé par ChatGPT doit être soigneusement vérifié par une personne réelle !

Les conseils pour utiliser ChatGPT en toute sécurité

N'utilisez que le site et l'application officiels de ChatGPT : Vous ne devez utiliser que le site web et l'application officiels de ChatGPT. Si vous craignez d'utiliser accidentellement un faux site ou une fausse application, mettez le site officiel de ChatGPT dans vos favoris afin d'y accéder plus facilement.

N'entrez jamais d'informations sensibles dans ChatGPT : Tout ce qui est entré dans ChatGPT est sauvegardé et stocké dans sa base de données, et si ChatGPT subit une violation de données, les informations privées que vous partagez avec ChatGPT pourraient se retrouver entre de mauvaises mains. C'est pourquoi il est crucial de ne pas télécharger de documents sensibles tels que des PDF juridiques ou des documents financiers dans ChatGPT.

Utiliser un compte anonyme : Si vous souhaitez minimiser les risques de sécurité lorsque vous utilisez ChatGPT, il est plus sûr d'utiliser un compte anonyme. Au début de cette année, ChatGPT a commencé à permettre aux personnes d'utiliser son chatbot instantanément, sans ouvrir de compte.

Vérifiez toujours les informations fournies par ChatGPT : Nous savons que ChatGPT peut parfois se tromper, il est donc important de se référer à des sources fiables et de faire des recherches externes pour confirmer l'exactitude du contenu produit par ChatGPT. De plus, faire vos propres recherches sur la base du contenu de ChatGPT clarifiera si ChatGPT est biaisé ou non dans la manière dont il dépeint ses informations.

Signalez les problèmes que vous rencontrez à OpenAI : Lorsque vous utilisez ChatGPT, vous pouvez rencontrer des problèmes qui doivent être résolus. Contactez directement OpenAI afin qu'ils puissent corriger les bugs rapidement.

Ne créez pas des mots de passe à l’aide de ChatGPT : Si ChatGPT crée des mots de passe pour vous et que les données de ChatGPT sont violées, un cybercriminel aura accès aux mots de passe qu'il a générés. Une autre raison importante pour laquelle vous ne devriez pas utiliser ChatGPT pour créer des mots de passe est qu'il peut générer les mêmes mots de passe pour plusieurs utilisateurs.

Plutôt que de prendre le risque que ChatGPT partage vos mots de passe ou en crée de faibles, il serait préférable d'utiliser un générateur et un gestionnaire de mots de passe. Un générateur de mots de passe peut créer des mots de passe forts et uniques en utilisant une combinaison aléatoire de lettres majuscules et minuscules, de chiffres et de symboles. Une fois créé, vous pouvez stocker votre mot de passe sécurisé dans un gestionnaire de mots de passe, un coffre-fort numérique destiné à conserver vos identifiants de connexion en toute sécurité.

Source : IT Channel - août 2024