



KEEPER®

Communiqué
de presse

Keeper Security intègre désormais un générateur de phrase de passe

Grâce aux phrases de passe générées et stockées de manière transparente dans Keeper, les utilisateurs bénéficient d'une protection renforcée en matière de cybersécurité, sans pour autant renoncer à la commodité.

Paris, le 16 avril 2024 – [Keeper Security](#), l'un des principaux fournisseurs de solutions zero trust et zero knowledge pour la protection des identifiants, des accès privilégiés et des connexions à distance, annonce aujourd'hui son nouveau générateur de phrases de passe. Le générateur de phrases d'authentification est une extension de Keeper Web Vault, qui sera bientôt disponible pour les appareils mobiles et sous forme d'extension de navigateur. La nouvelle version contient également une mise à jour du générateur de mots de passe existant. Celui-ci offre aux utilisateurs des options supplémentaires pour répondre à des exigences spécifiques en matière de mots de passe. Outre la possibilité d'utiliser des lettres majuscules, des chiffres et des symboles, il est désormais possible de choisir des symboles spécifiques qui peuvent être ajoutés en fonction des exigences du site web pour lequel le mot de passe est créé.

« Les nouvelles mises à jour de l'intégration des phrases de passe et du générateur de mots de passe de Keeper permettent aux utilisateurs de créer des phrases de passe et des mots de passe hautement sécurisés pour protéger leurs comptes en ligne », explique Craig Lurey, CTO et cofondateur de Keeper Security. « Ces nouveautés renforcent non seulement la sécurité des utilisateurs privés et professionnels, mais simplifient également l'expérience utilisateur, ce qui est en accord avec notre volonté de proposer des solutions de cybersécurité faciles à utiliser, qui améliorent la sécurité et augmentent la productivité ».

La protection des informations sensibles est essentielle dans le monde en réseau d'aujourd'hui. L'utilisation généralisée de mots de passe faibles et répétitifs fait que de nombreux individus et entreprises ne sont pas suffisamment protégés contre les cybermenaces de plus en plus répandues et sophistiquées. Les phrases de passe présentent plusieurs avantages par rapport aux mots de passe traditionnels - elles sont notamment plus longues et intrinsèquement plus complexes, mais plus faciles à retenir.

Les phrases de passe sont composées de plusieurs mots mis bout à bout. Plus une phrase de passe contient de mots, plus elle est longue et plus elle est difficile à craquer pour les cybercriminels. Les mots de passe, en revanche, sont composés d'une série de caractères. Pour sécuriser correctement un compte, il est donc recommandé que les mots de passe comportent au moins 16 caractères et contiennent une combinaison aléatoire de lettres, de chiffres et de symboles. Cependant, comme les gens essaient souvent de se souvenir des mots de passe classiques, ceux-ci sont souvent faibles ou utilisés pour plusieurs comptes.

Le nouveau générateur de phrases de passe de Keeper est intégré au générateur de mots de passe existant et permet aux utilisateurs et aux administrateurs de choisir lequel des générateurs doit être privilégié ou imposé à l'organisation. Le générateur de Keeper utilise la liste de mots recommandée par l'[Electronic Frontier Foundation](#) , soit 7 776 mots (nettoyés pour éliminer tous les mots choquants). Les utilisateurs peuvent générer des phrases de passe cryptographiquement sécurisées adaptées à leurs besoins spécifiques, par exemple le nombre de mots qu'elles contiennent, le type de séparateur utilisé et si elles contiennent des chiffres et des lettres majuscules. Le processus de création et de stockage des phrases de passe avec Keeper est le même que pour les mots de passe et les passkeys, et il offre une expérience utilisateur transparente.

Les principaux avantages du générateur de phrases de passe sont les suivants :

- **Sécurité accrue** - Crée des phrases de passe fortes et uniques qui résistent aux [attaques par force brute et aux cyber-menaces liées aux mots de passe](#).
- **Options de personnalisation** - Les phrases de passe peuvent être adaptées aux exigences de sécurité, y compris la longueur, les types de caractères et la complexité.
- **Une approche simplifiée** - Une interface utilisateur intuitive permet aux utilisateurs de créer facilement et de manière transparente les phrases de passe pour leurs comptes.

Avec l'intégration du générateur de phrase de passe, Keeper donne à ses utilisateurs les outils dont ils ont besoin pour garder une longueur d'avance sur les acteurs malveillants et les cyber-menaces en évolution.

Pour en savoir plus sur l'intégration du générateur de phrases de passe de Keeper et les avantages qu'il offre tant aux particuliers qu'aux entreprises, cliquez [ici](#).

###

A propos de Keeper Security:

Keeper Security transforme la cybersécurité pour les personnes et les organisations du monde entier. Les solutions de Keeper, abordables et faciles à utiliser, sont construites sur la base d'une sécurité Zero Trust et Zero Knowledge pour protéger chaque utilisateur sur chaque appareil. La solution de gestion des accès privilégiés de nouvelle génération Keeper se déploie en quelques minutes et s'intègre de manière transparente à n'importe quelle stack technologique pour prévenir les violations, réduire les coûts du service d'assistance et garantir la conformité. Des millions de personnes et des milliers d'organisations font confiance à Keeper, le leader en matière de gestion de mots de passe et de passkeys, de gestion des secrets, d'accès privilégié, d'accès à distance sécurisé et de messagerie chiffrée.

Pour en savoir plus, visitez le site KeeperSecurity.com

Suivre Keeper: [Facebook](#) [Instagram](#) [LinkedIn](#) [X](#) [YouTube](#)

Contact Presse :

Christelle Klein :

06 63 97 01 67

cklein@hl-com.com