

N'oublie plus tes mots de passe



SOMMAIRE

● Introduction	Page 1
📄 Fuite de données	Page 2
✅ Complexité du mot de passe	Page 3
⚡ Gestionnaire de mots de passe	Page 4
💡 Astuce pratique	Page 5

● Introduction

Utiliser le même mot de passe partout, ce n'est pas une bonne idée. C'est une faille importante dans la protection de tes données. Un gestionnaire de mots de passe, c'est donc super pratique pour t'en sortir. Parce que oui, retenir tous ses mots de passe, c'est mission impossible.

Dans cet ebook, on va d'abord voir comment vérifier si ton adresse email (ou tes mots de passe) ont fuité. Ensuite, je te montre comment utiliser un gestionnaire de mots de passe gratuit et fiable. Et pour finir, je te partage une astuce simple pour avoir un mot de passe différent sur chaque site, sans jamais les oublier. De quoi tester plein de nouveaux outils sans te prendre la tête.



Fuite de données

HaveIBeenPwned vérifie et collecte les données qui ont fuité sur le dark web, des forums et d'autres sources publiques. L'outil a été créé par Troy Hunt, un expert australien en cybersécurité. Son équipe s'assure que les fuites sont bien réelles en vérifiant l'authenticité des données.

Have I Been Pwned

Check if your email address is in a data breach

Check

Using Have I Been Pwned is subject to the [terms of use](#)

L'outil est vraiment simple à utiliser : tu peux faire une recherche avec une adresse email, ou même avec un mot de passe. Pas besoin de t'inscrire ni de payer quoi que ce soit pour faire la vérification.

8

Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

 Stay Protected

Get notified when your email appears in future data breaches

Notify Me

Twitter (200M)

In early 2023, over 200M records scraped from Twitter appeared on a

Jan
2021

✔ Complexité du mot de passe

Ce n'est plus un secret : plus ton mot de passe est long, plus il est difficile à deviner. Mais ce n'est pas tout. Il vaut mieux aussi ajouter des chiffres, des lettres majuscules, des caractères spéciaux, etc.

Plus ton mot de passe est complexe, plus il sera difficile à pirater.

Combien de temps faut-il à un pirate pour trouver votre mot de passe 2025

12 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	57 minutes	2 heures	4 heures
6	Instantané	46 minutes	2 jours	6 jours	2 semaines
7	Instantané	20 heures	4 mois	1 an	2 ans
8	Instantané	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3k ans	11k ans
10	1 jour	40 ans	41k ans	238k ans	803k ans
11	1 semaine	1k ans	2M ans	14M ans	56M ans
12	3 mois	27k ans	111M ans	917M ans	3Md ans
13	3 ans	705k ans	5Md ans	56Md ans	275Md ans
14	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans
15	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans
16	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans
17	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans
18	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans



Hive Systems

hivesystems.com/password

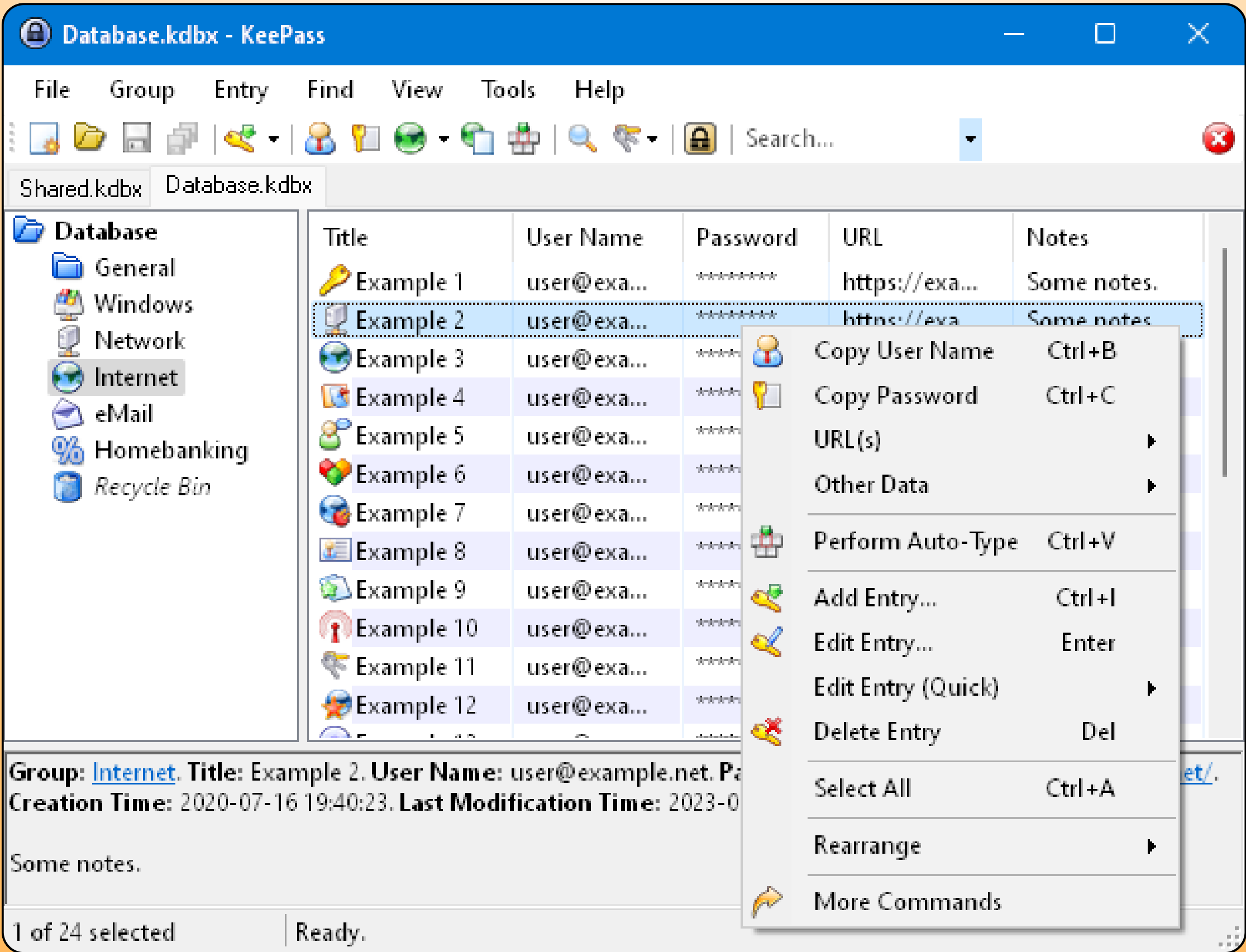
Estimation du temps pour trouver votre mot de passe.

⚡ Gestionnaire de mots de passe

Plus un mot de passe est complexe, plus c'est galère de s'en souvenir. Et noter tes mots de passe dans un fichier texte ou un cahier, c'est vraiment à éviter. Surtout si tu mets le nom du site juste à côté . Une bien meilleure option : Keepass



C'est un gestionnaire de mots de passe gratuit et open-source, qui te permet de sauvegarder tous tes mots de passe dans une base de données chiffrée (au format .kdb ou .kdbx). L'outil est léger, fiable et sécurisé, avec un chiffrement solide de type AES-256 (Advanced Encryption Standard).



Capture d'écran de KeePass

💡 Astuce pratique

Je vais te partager une astuce que j'utilise depuis des années pour avoir un mot de passe différent sur chaque site... Et m'en souvenir à chaque fois, sans me prendre la tête .

- Commence par définir une base de mot de passe.
- Complexifie un peu, ajoute un chiffre et des caractères spéciaux.
- Ajoute ensuite le nom du site à la fin.

Résultat : un mot de passe complexe et **différent sur chaque site** !

innospirá

Base standard	InnoSpira	9 caractères
Base complexe	Inn05pir@!	10 caractères
Base complexe + site	Inn05pir@!gmail	15 caractères
Base complexe + site complexe	Inn05pir@!gmail5gl*	19 caractères

COMPLEXITÉ
↓

Si tu as aimé ce support, n'hésite pas à m'encourager en **laissant un like et/ou un commentaire** ! Ton soutien me motive à créer davantage de contenus similaires 😊

Jérémie - Juillet 2025

