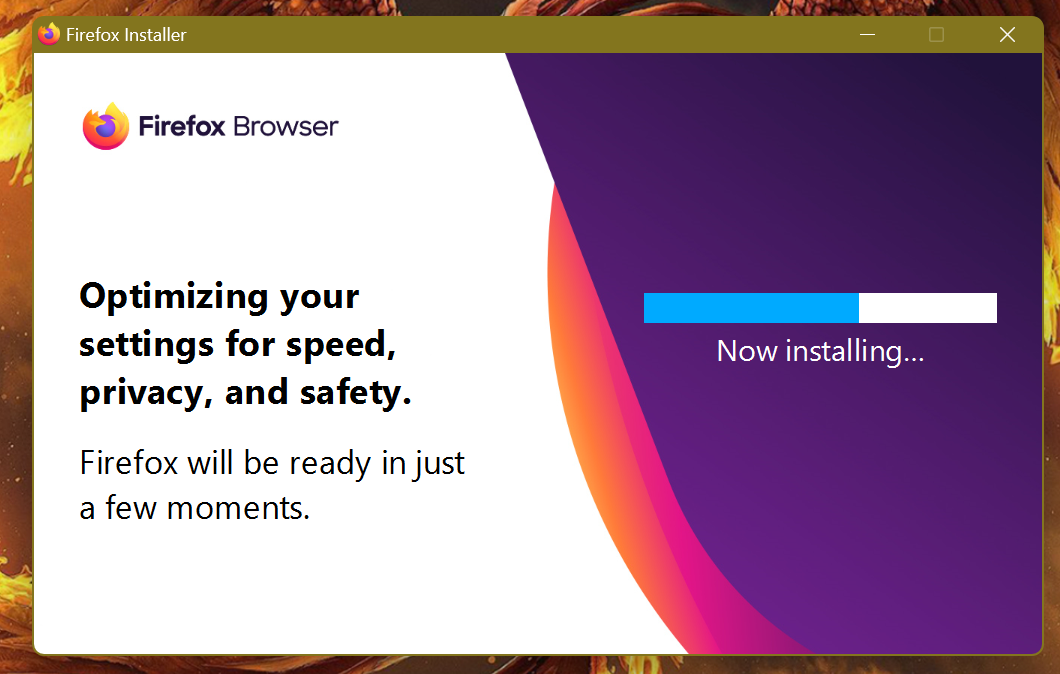
**TP – Gestionnaire de mots de passe**

Sécuriser les équipements et les usages des utilisateurs

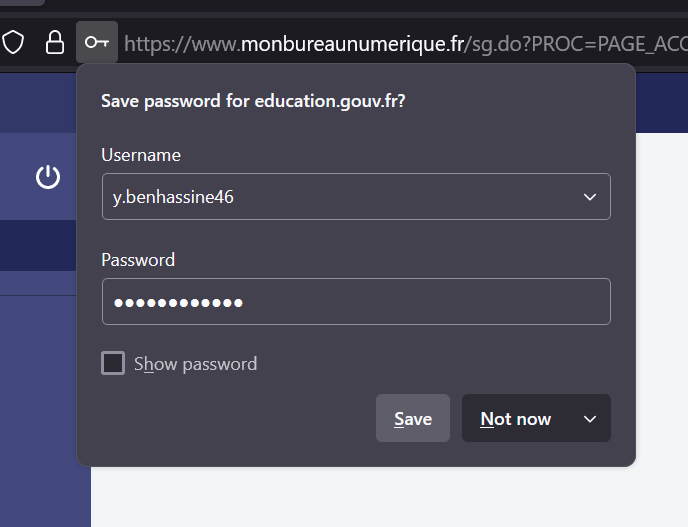
1. **Gestionnaire de mots de passe Firefox**



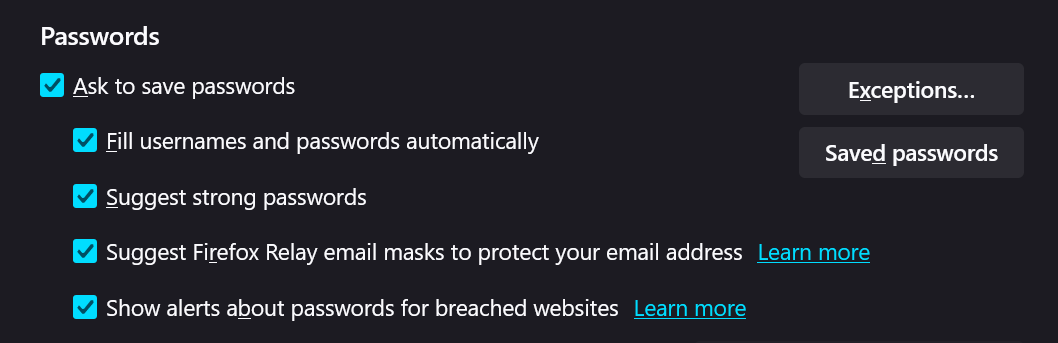
Je me connecte



J’enregistre le mot de passe



Saved passwords





5. L'oeil de horus permet de voir le mot passe en clair

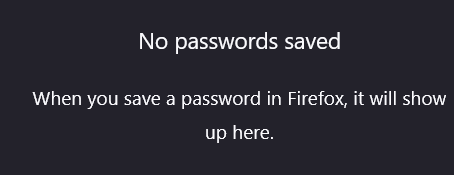
6. Cela représente un grand risque de sécurité

7. On peut modifier le mot de passe, mais cela ne modifie pas le vrai mot de passe qui permet d'accéder au compte, ici on modifie seulement le mot text enregistré

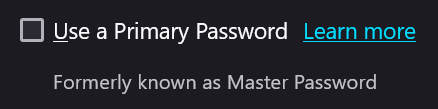
| Information sur username | "usernameField":"j\_username"  "encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECPLW4StYpzASBBBEeHLbGSpnGxS6PriH4WNT" |
| --- | --- |
| Informations sur mdp | "passwordField":"j\_password"  "encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECN6MzG2ajVEnBBDtrHHlesM54ZRMbEvPG/gb" |
| Autres informations utiles | "Guid":"{Aafab4d8-1b9b-4972-b056-b5bbd1d33ce8}",  "encType":1,  "timeCreated":1707287336624,  "timeLastUsed":1707287336624,  "timePasswordChanged":1707287336624,  "timesUsed":1,  "syncCounter":1,  "everSynced":false,  "encryptedUnknownFields":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECLbBPq/cWqF/BAiwXsr5S5UkAw=="}],  "potentiallyVulnerablePasswords":[],  "dismissedBreachAlertsByLoginGUID":{},  "version":3} |

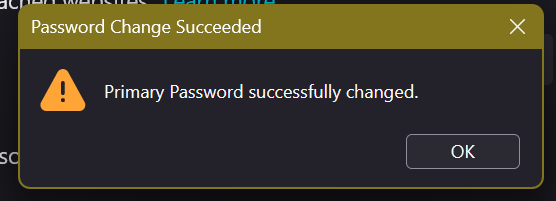
Les données sensibles comme le mot de passe et le nom d’utilisateur n’apparaissent pas en clair, mais en chiffré

Identifiants supprimés



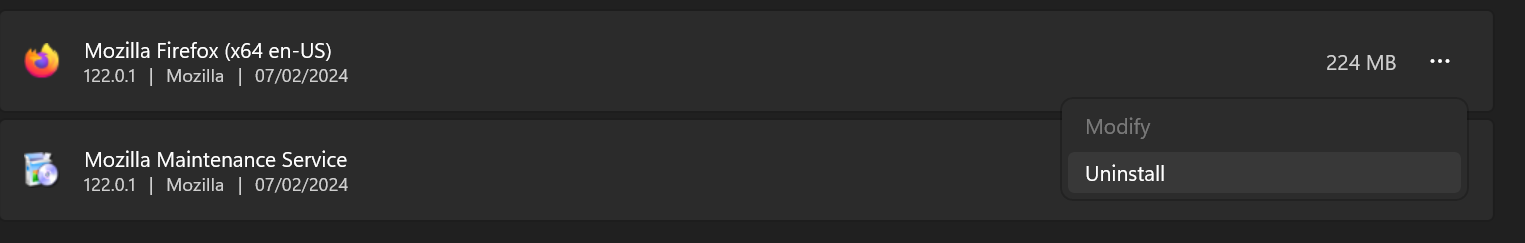
Mot de passe principal



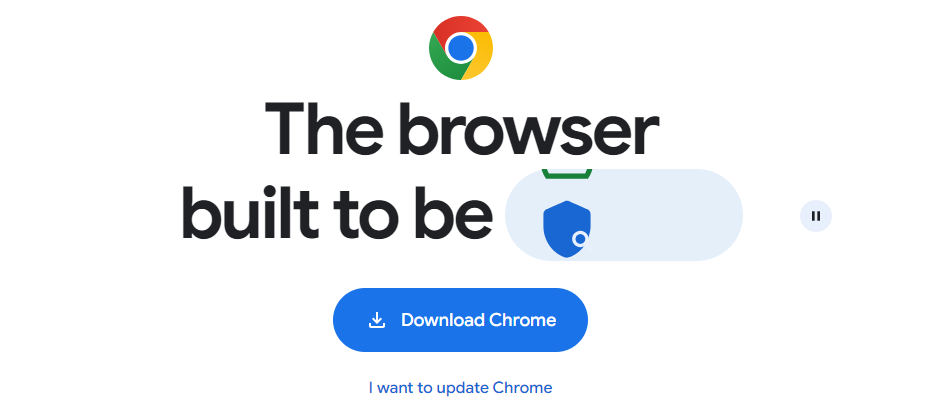


Le mot de passe principal, autrement appelé (master password), permet d'accéder à tous les comptes (ayant des mot de passes et identifiants différents) avec un seul mot de passe.

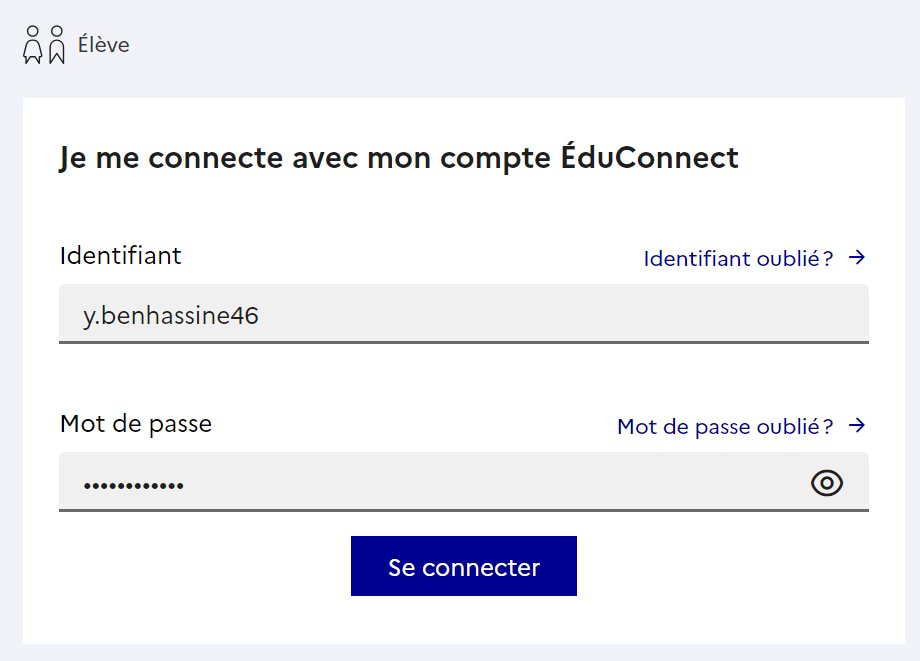
Les mots de passes principaux sont souvent utilisés dans les gestionnaires de mots de passes (où on enregistre ses mot identifiants).



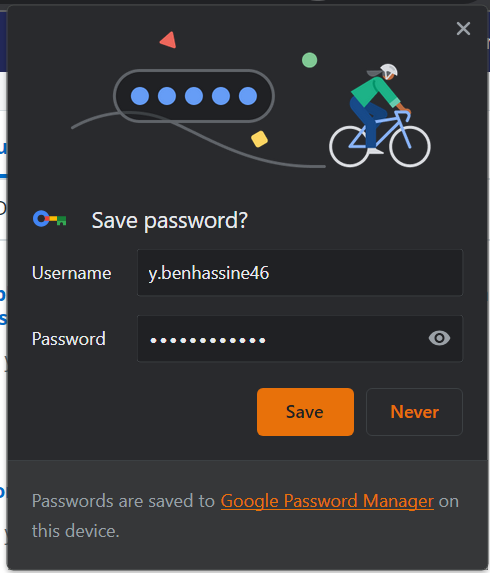
1. **Gestionnaire de mots de passe de chrome**



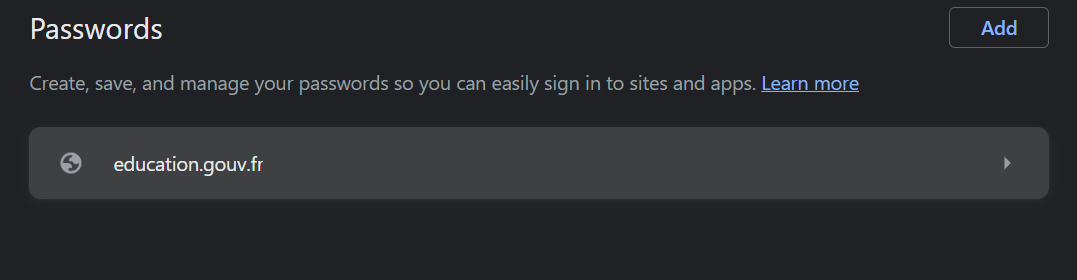
Je me connecte à mon compte



J'enregistre le mot de passe

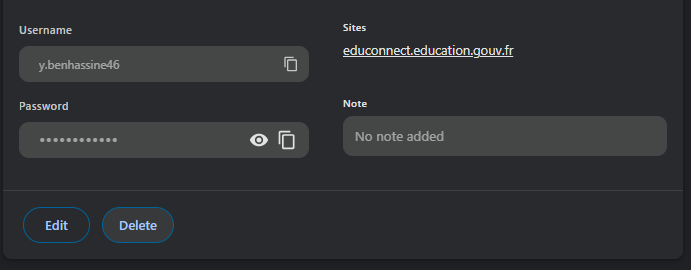


Le password manager (gestionnaire de mots de passe)

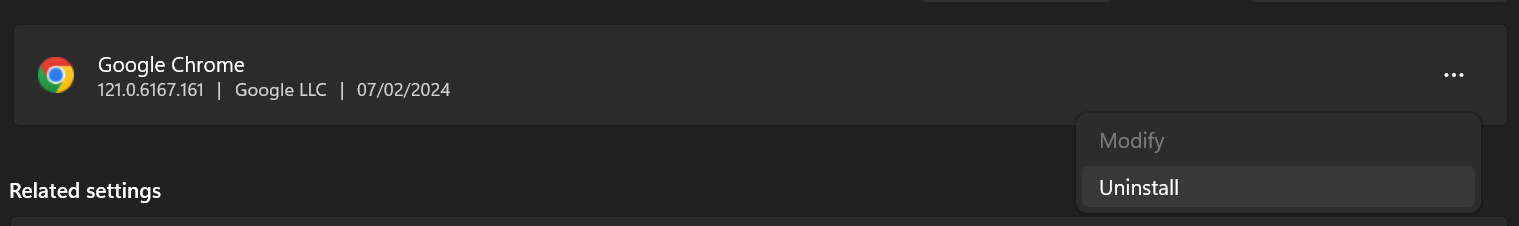
****

Avant de pouvoir accéder aux mots de passe, l’utilisateur doit saisir le code pin de son système, ou alors dans mon cas, être reconnu par le système de reconnaissance faciale, l’essentiel c’est que l’utilisateur ne peut pas directement accéder aux mot de passes et pouvoir les visualiser ou les modifier.

Delete

****

Je désinstalle chrome



1. **Gestionnaire de mots de passe Keepass**

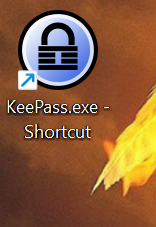
**Objectif :** utiliser le gestionnaire de mots de passe Keepass

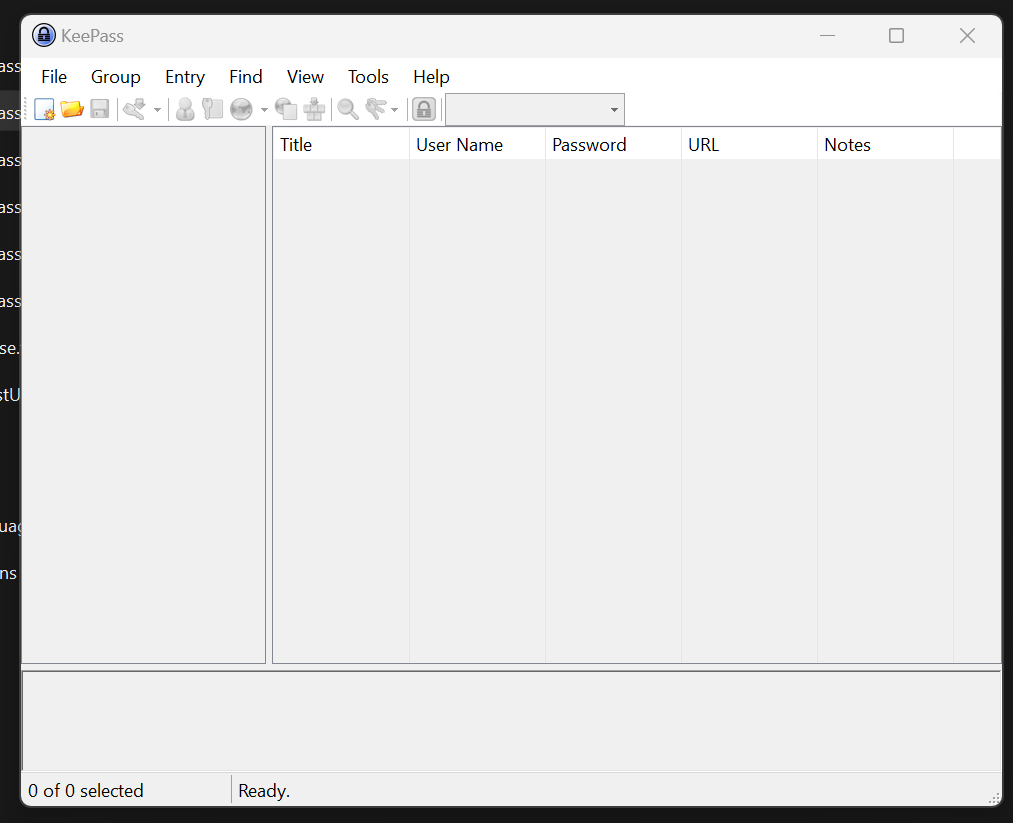
KeePass est un gestionnaire de mots de passe, certifié par l’ANSSI

Lien d’installation: <https://keepass.info/download.html>

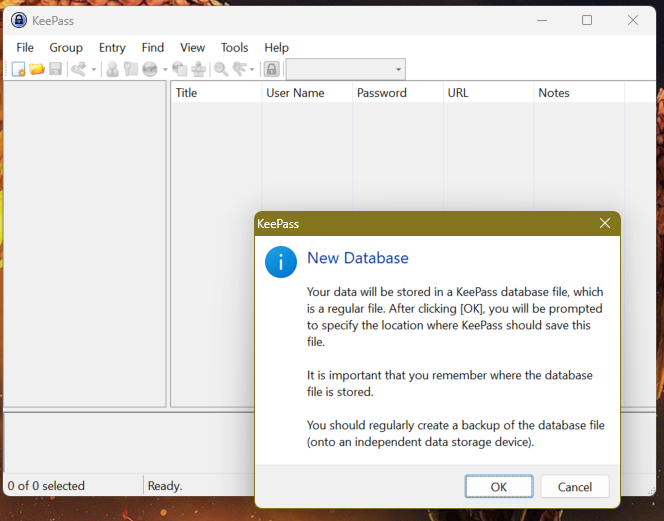
Lien vers video CNIL: <https://www.youtube.com/watch?v=XTnDKJl1zOQ>

Raccourci vers le programme

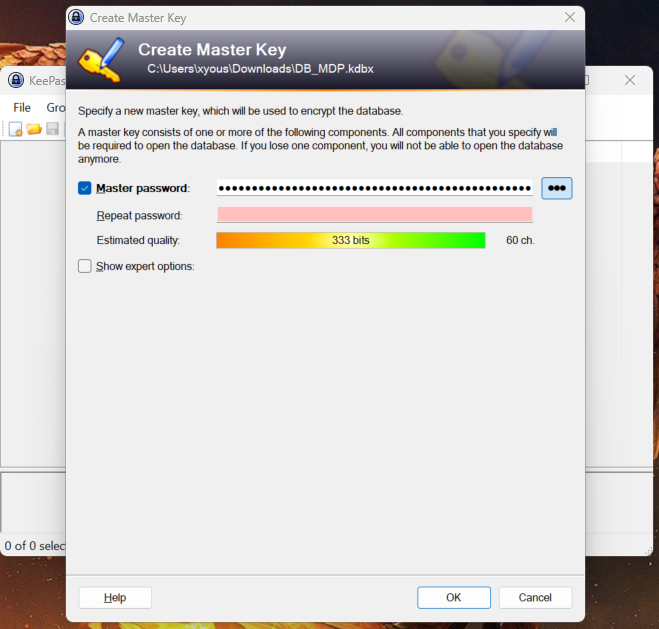




Nouvelle base de données de mots de passe

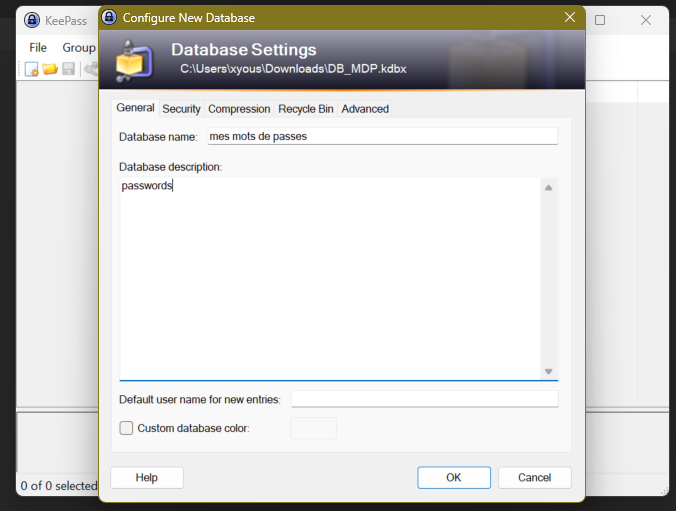


On met un mot de passe principal (master key)

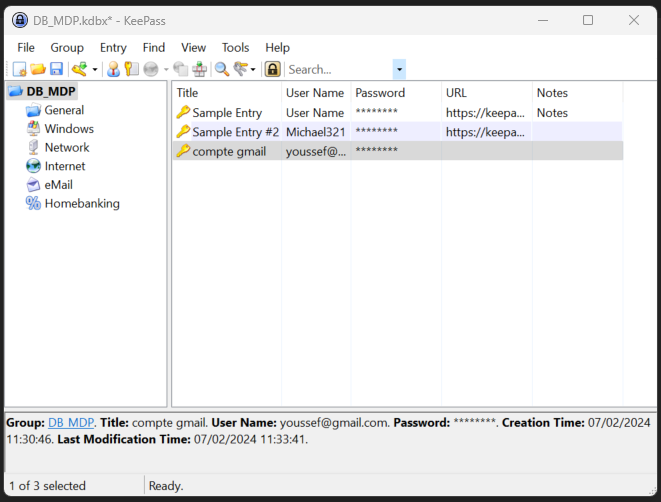


La clé

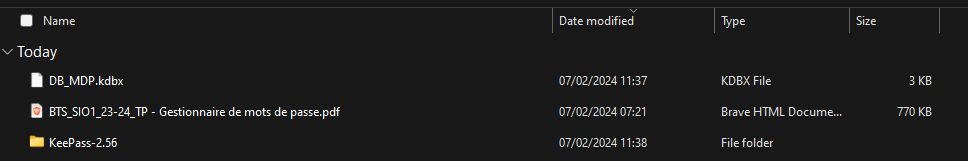




Si l’on veut se connecter, on copy/paste, les identifiants à partir de l’application KeePass

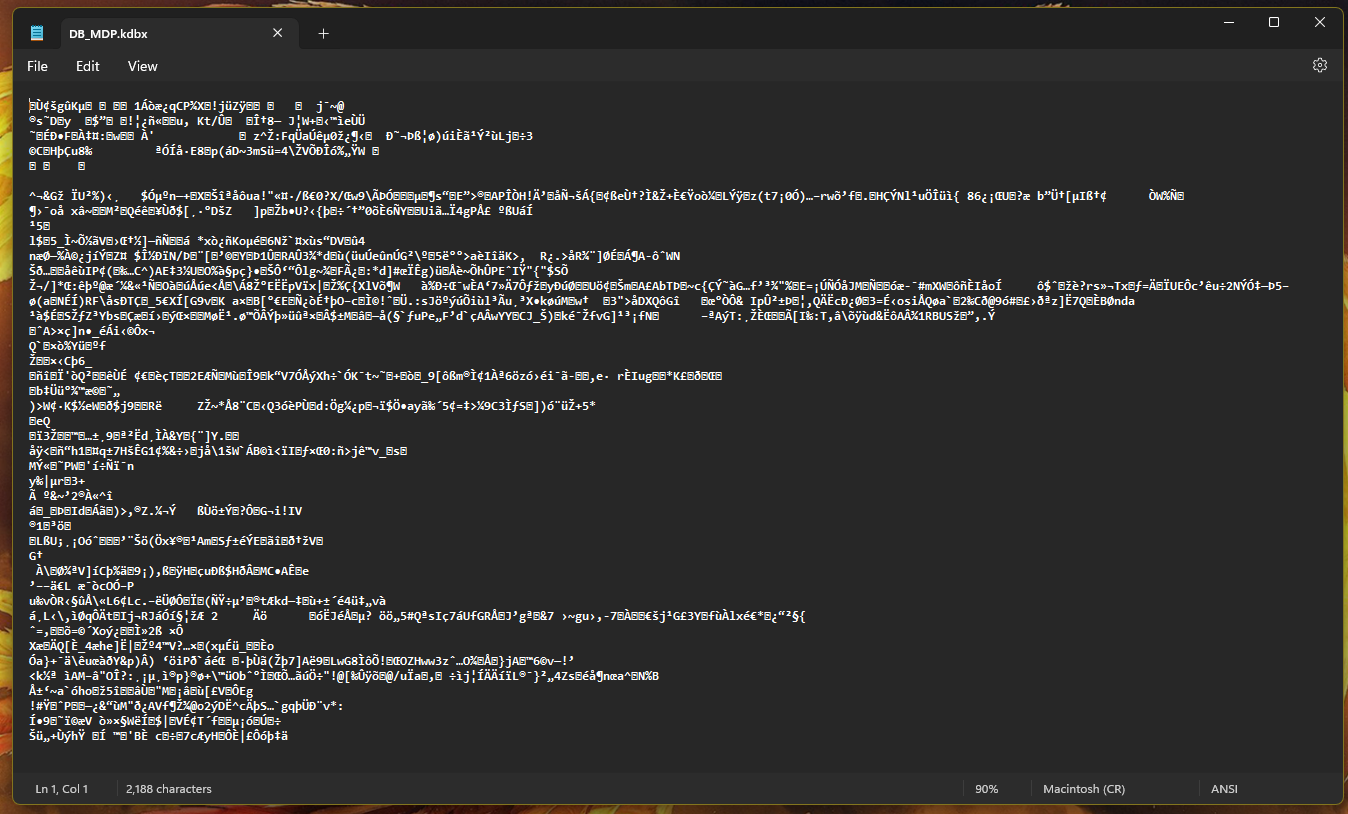


J’accède au fichier de la base de données

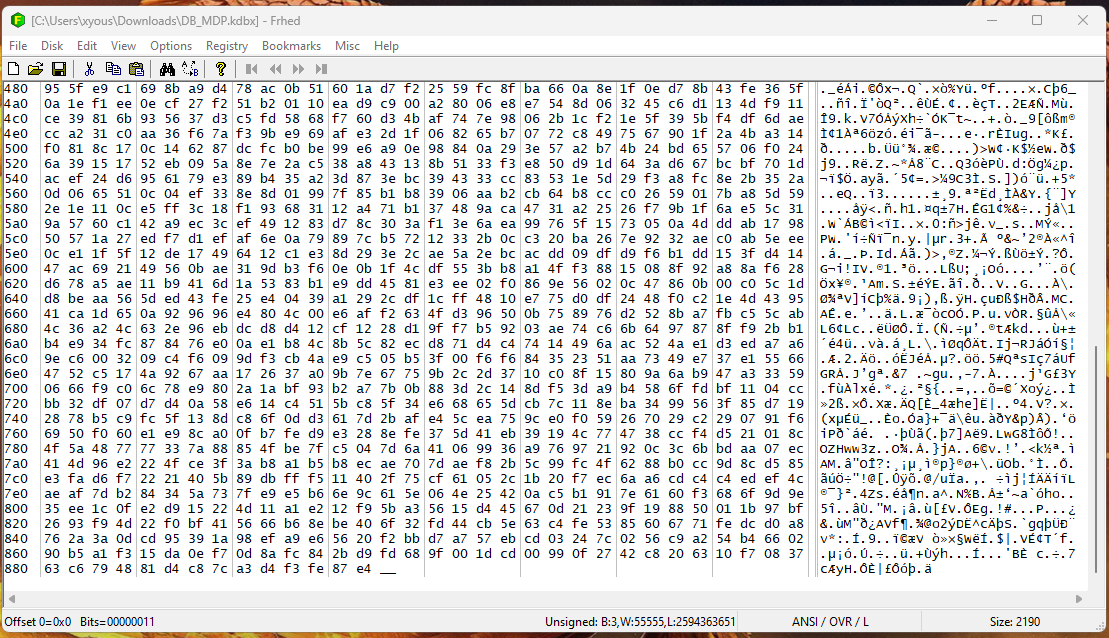


Le contenu du fichier de base de données est très illisible

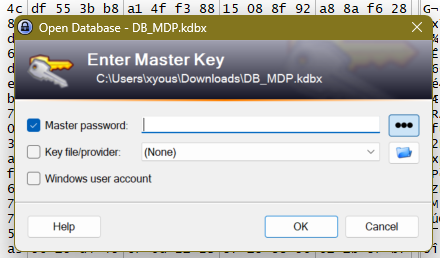
notepad:

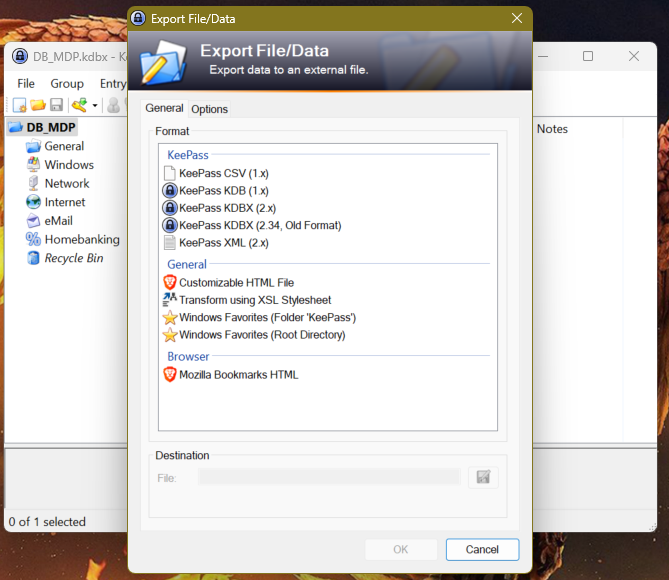


Frhed:



Je rouvre le fichier de la base données





Le choix d’exporter permet de réinstaller le logiciel sur une autre machine ou d’avoir accès à tous les mots de passes accumulés sur une longue période sans avoir à ressaisir toutes les entrées, cet outil facilite cette tâche.

**Avantages d'utiliser Frhed comparé à Firefox**

Frhed permet un contrôle total sur la gestion des mots de passe, permet une sécurité et confidentialité supérieure à celle proposé par mozilla firefox, néanmoins nécessite une connaissance informatique pour pouvoir l’utiliser, n’est pas très accessible au utilisateurs non techniques.

En conclusion, firefox est facile d’utilisation sans sécurité. Frhed est plus technique mais beaucoup plus sécurisé.