Eskimon

Zeste de savoir

Utiliser un gestionnaire de mot de passe

21 décembre 2018

Table des matières

1. Introduction

Dans ce tutoriel, je vais vous présenter de la manière la plus imagée et la plus simple possible un principe de sécurité informatique facile à mettre en place, que tout le monde, même sans connaissance de l'outil informatique sera en mesure de mettre en place ! Le but étant de vous aider à mettre en place une petite sécurité supplémentaire pour améliorer la protection de vos services en ligne et de votre vie privée numérique.

i Prérequis

Aucune connaissance informatique n'est requise pour suivre ce tuto. En revanche, un peu de motivation et de bonne volonté pour mettre en pratique les quelques conseils proposés ici seront les bienvenus .

2. Dans la vraie vie, comment ça se passe ?

Dans la vie de tous les jours, votre trousseau de clé pour accéder à votre logement, véhicule, bureau ressemble plutôt à celui de gauche ou à celui de droite ?

FIGURE 2. – Des clés… de différentes forces !

Je pense qu'on est d'accord pour dire que la majorité répondra celui de droite (même mes enfants, qui galèrent à parler, préfèrent le trousseau de droite à celui de gauche, comme quoi !).

Et utilisez-vous la même clé pour la porte d'entrée, la voiture, la boîte aux lettres ou le cabanon du jardin ?

Eh bien fondamentalement la sécurité en ligne c'est exactement la même chose, sauf qu'une clé s'appelle un mot de passe !

Vous pouvez utiliser juste quelques clés pour tout vos services en ligne (email, réseaux sociaux, sites marchands, banques, etc) ou bien utiliser une et une seule clé pour chacun des services. Tout comme vous utilisez déjà une clé pour votre porte d'entrée, une pour votre vélo, une autre pour le garage, etc.

Et sinon, vos clés, elles sont plutôt en « plastique tout mou avec jusque quelques trous et bosses » ou plutôt «métal costaud avec des creux/bosses de différents niveaux voire des trous de différentes diamètres» ?

J'imagine la seconde option. C'est ce qu'on appelle une protection «forte». Vous avez peut-être déjà croisé ce terme lorsque vous vous êtes inscrits sur un site internet. Si vous essayez le mot de passe <abc123> le site vous répondra que le mot de passe est faible (clé en plastique). Alors que si votre mot de passe ressemble plutôt à <qQ6jR157Ms_$cS~/> le mot de passe sera qualifié de «fort» (clé en métal).

Et tout le secret est là. Utiliser des mots de passe **forts** et **différents** pour chacun de vos services, comme vous utilisez une clé différente pour chacune de vos serrures.

Alors vous allez sûrement me répondre :

> ? Tu es bien gentil, mais chez moi mes clés je les promène sur un seul trousseau. Comment tu veux que je me rappelle de tout plein de mots de passe incongrus ?

Rassurez-vous, je ne vous demande pas de devenir champion de la mémoire. Nous allons juste utiliser un outil qui fera ça très bien pour nous : un gestionnaire de mot de passe.

3. Un gestionnaire de mot de passe, comment ça marche ?

Le principe d'un gestionnaire de mot de passe est très simple. C'est un coffre-fort qui contiendra tous vos mots de passe. Et quand j'utilise le mot «coffre-fort», c'est presque littéral .

En effet, il vous suffit d'imaginer que l'internet représente tout l'espace à l'extérieur de votre logement et que votre maison soit votre ordinateur. Ce que je vous propose, c'est de mettre chez vous un coffre-fort qui contiendra tous vos mots de passe. Ce coffre-fort sera impossible à ouvrir, sauf par vous, car vous serez la seule personne à en avoir la combinaison. Une fois ouvert, vous pourrez alors prendre le mot de passe qui vous intéresse pour accéder au site internet auquel vous souhaitez vous connecter. Vous pourrez aussi évidemment ajouter de nouveaux mots de passe dedans pour compléter votre trousseau de clé numérique.

> *i* Ce coffre-fort sera uniquement sur votre ordinateur. Vous n'y aurez donc pas accès depuis un autre ordinateur. Cependant, dans la dernière partie de ce tutoriel je vous expliquerais comment le synchroniser entre différents appareils en toute sécurité !

Vous vous en doutez peut-être, pour que cette stratégie fonctionne il faut que le code de votre coffre-fort soit robuste. Ce sera là le seul effort à faire : trouver et se souvenir d'un mot de passe *fort* pour sécuriser votre coffre. Avantage, dorénavant ce sera le seul mot de passe dont vous devrez vous souvenir. Mais nous y revenons juste après une petite pause pour parler chiffres et actualités.

4. Interlude?? Parlons chiffres et actualités

Quelque chose est important à comprendre : Utiliser un seul mot de passe par service est primordial. En effet, si vous utilisez le même mot de passe-partout, alors il suffit qu'un seul site internet ne se fasse pirater pour compromettre l'ensemble de vos accès à d'autres services/sites internet. En revanche, si vous utilisez un mot de passe unique par service, l'attaque de l'un d'entre eux et le vol de sa base de donnée n'impactera pas votre sécurité sur les autres sites.

A titre d'exemple, voici quelques évènements majeurs sur la dernière décennie :

En mai 2016, le célèbre site de réseau professionnel «LinkedIn» a vu 164 millions de couples email/mot de passe révélé suite à une attaque.

Octobre 2013, l'éditeur de logiciels professionnels de graphisme et d'un célèbre lecteur pdf, Adobe, s'est fait attaquer. 153 millions d'emails, de mots de passe chiffrés (mais avec leurs questions types «*Quel est le nom de votre premier animal*») sont partis dans la nature.

Mai 2015, le site de rencontre américain *Adult Friend Finder* s'est fait pirater. 4 millions de comptes sont alors subtilisés avec notamment les identités des personnes, leur situation géographique, leur orientation sexuelle et probablement d'autres données sur leur historique d'utilisation du service. Dans la même veine et posant les mêmes soucis sur la vie privée des utilisateurs, les sites *Beautiful People* (2015, 1.1 millions de comptes volés), *JustDate* (2016, 24 millions de comptes) et *Mate1* (2016, 27 millions de comptes) ont eux aussi subits des attaques.

Mai 2014, l'éditeur d'antivirus Avast ! s'est fait volé 423 000 informations de comptes (nom de profil, email et mot de passe chiffré). Apprécions l'ironie, même un spécialiste des attaques informatiques n'est pas infaillible.

En septembre 2014, 5 millions de comptes Gmail étaient mis en vente au marché noir.

Et un des plus gros sites au monde, Facebook, s'est aussi vue attaqué (mais sans vol d'informations) en septembre 2018. À la louche 50 millions de comptes ont été piratés.

Toutes ces données proviennent du site (en anglais) : https ://haveibeenpwned.com/ . Ce site propose aussi un formulaire vous permettant de vérifier si votre email a été retrouvé parmi des comptes volés suite à des attaques.

Avez-vous remarqué ? Tous ces sites sont des mastodontes de l'informatique et de l'internet. Ce sont des sites dont le business se fait 100% via l'outil informatique. Et pourtant, aucun n'est infaillible. Je ne mentionnerais même pas les plus petits sites n'ayant pas les moyens de faire des audits de sécurité complets.

La sécurité à 100% n'existe pas. Il y aura toujours une brèche et les pirates rivalisent d'ingéniosité tous les jours pour y parvenir. Une fois les données en leurs mains, ils ne leur faut que très peu de temps pour lancer une batterie d'outils qui testera les couples courriels/mot de passe sur les services en ligne les plus connus.

Une fois que la brèche a eu lieu il est trop tard, le compte est corrompu. Cependant, les utilisateurs (vous !) peuvent mettre en place des solutions pour éviter la propagation. Utiliser des mots de passe différents sur chacun des sites en est une.

5. Place à la pratique, utilisons ce fameux gestionnaire de mot de passe (KeeWeb)

J'espère que rendu à ce point de la lecture, vous avez cerné les enjeux et l'intérêt d'utiliser des mots de passe **fort** et **uniques** sur chacun des services en ligne que vous fréquentez.

Comme je vous l'expliquais au début du tutoriel, l'objectif est de n'avoir à retenir qu'un seul mot de passe, le plus efficace possible (tant en termes de facilité à le retenir, que de difficulté à le deviner pour un étranger). Tous les autres mots de passe que vous utiliserez pour des sites en

ligne seront dorénavant générés automatiquement, complètement aléatoirement, pour être fort et unique.

5.1. Le logiciel utilisé : « KeeWeb »

Allons-y, mettons en oeuvre tout cela.

Le logiciel que je vous propose d'utiliser s'appelle KeeWeb. J'ai choisi de vous présenter ce dernier pour plusieurs raisons :

- Il est gratuit ;
- Il est disponible en français ;
- Il fonctionne sur tout les systèmes (Mac, Windows, Linux) ;
- Il en existe une version en ligne si vous ne pouvez pas installer de logiciels sur votre ordinateur (dans ce cas votre coffre-fort devra être synchronisé, j'y reviendrais) ;
- Enfin, il est *open-source*. Cela signifie que n'importe qui peut étudier son comportement et pourquoi pas contribuer pour corriger des bugs ou le rendre meilleur. Cette visibilité publique permet aussi de garantir que le logiciel ne nous espionne pas à notre insu.

Vous pouvez le trouver à l'adresse suivante : https ://keeweb.info/ . Sur ce site, vous pouvez télécharger le fichier pour installer sur votre ordinateur ou utiliser la version en ligne directement, à vous de voir ! Je vous laisse l'installer si vous choisissez cette option avant de passer à la suite de la lecture.

5.2. L'interface de KeeWeb

Lorsque vous démarrez le logiciel, vous vous retrouvez alors devant une fenêtre vous demandant d'ouvrir un fichier. Comme nous n'avons pas encore de coffre-fort, sélectionnez l'option «Nouveau». Les prochaines fois, votre coffre-fort (aussi appelé «base de données de mot de passe») sera proposé directement sur cet écran.

5. *Place à la pratique, utilisons ce fameux gestionnaire de mot de passe (KeeWeb)*

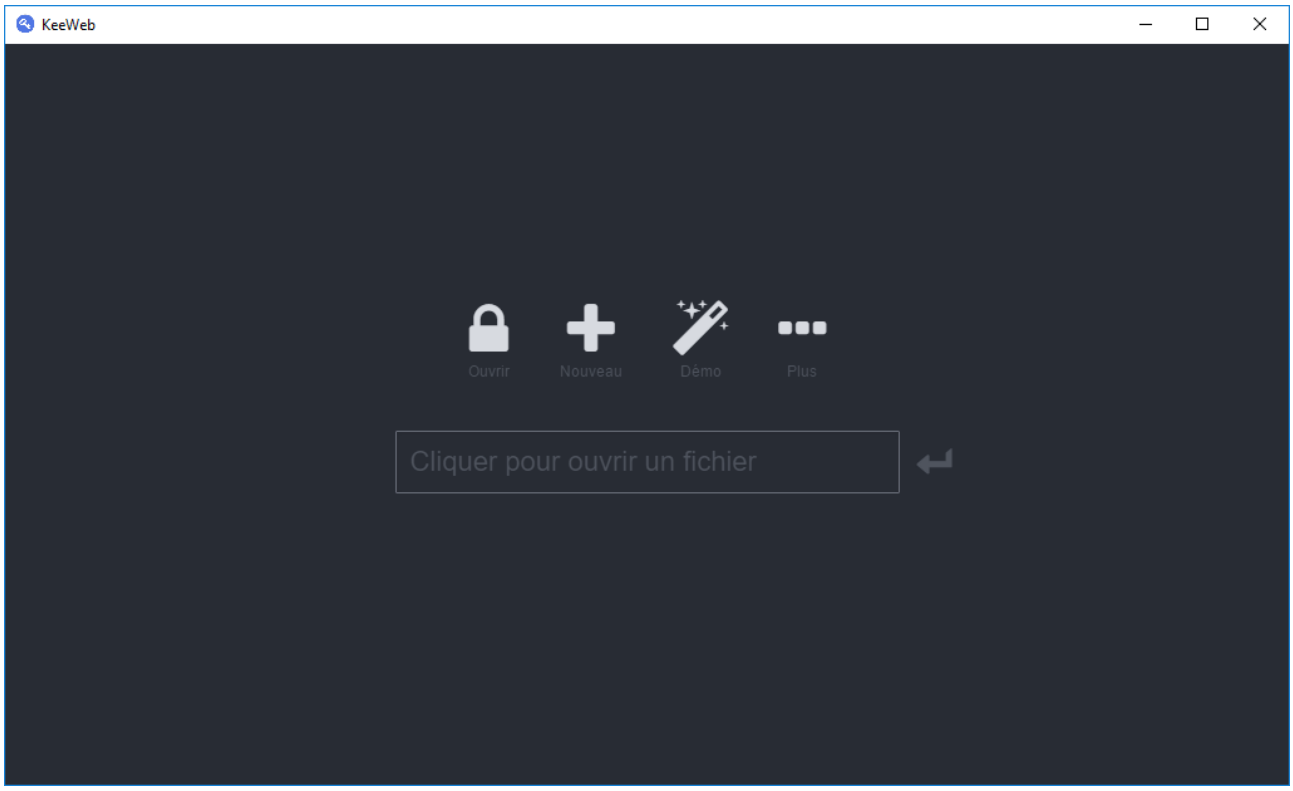

FIGURE 5. – Accueil de KeeWeb

Vous vous retrouvez alors dans l'interface de KeeWeb qui vous résume les différentes parties de l'écran :

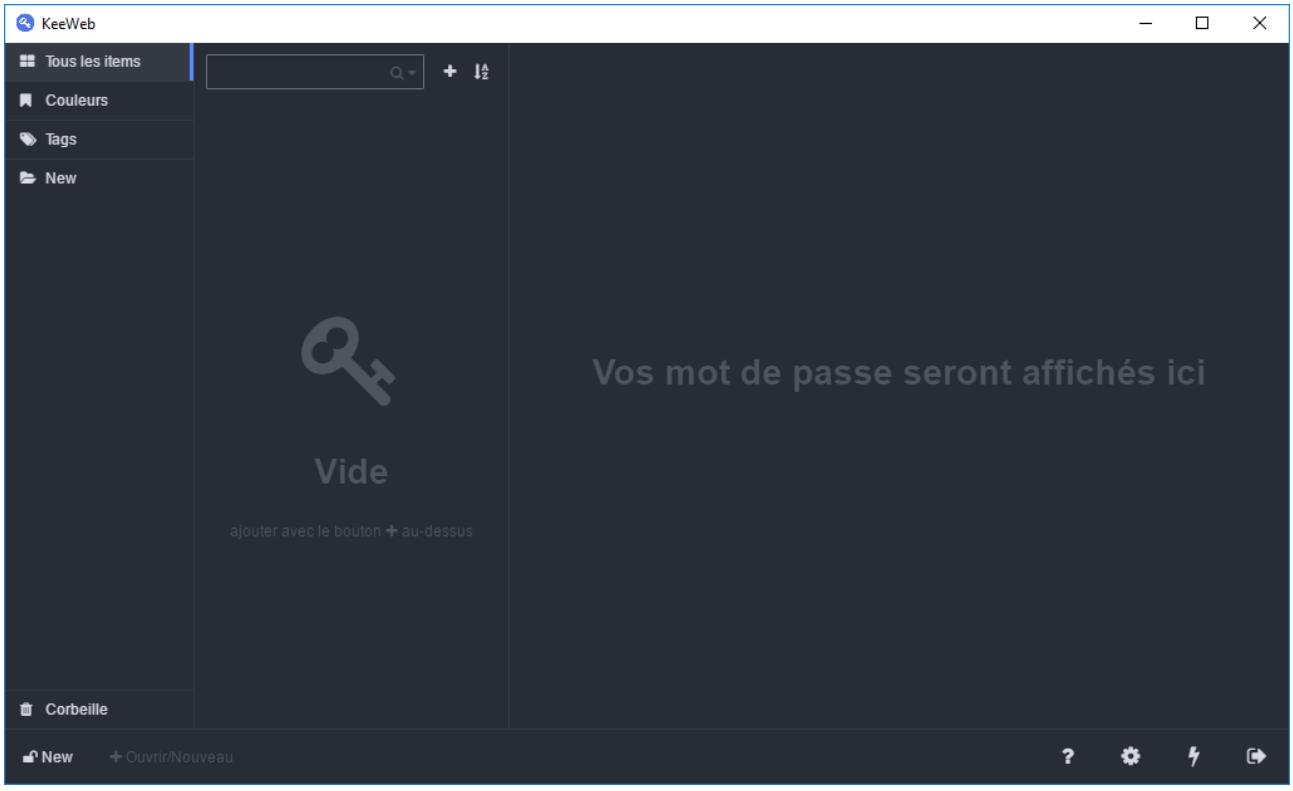

FIGURE 5. – L'interface de KeeWeb

Cette interface se découpe en trois colonnes. De gauche à droite on trouve :

— Un menu permettant de classer nos mots de passe ;
— Une colonne vide qui contiendra une liste des mots de passe ;
— Une fenêtre (vide pour le moment) qui permettra de voir et éditer un mot de passe en particulier.

Sans plus attendre, créons notre premier mot de passe ! Pour cela, cliquez sur le bouton tout en haut en forme de [ ], à côté du champ de recherche, dans la deuxième colonne, puis sélectionnez «Nouvelle entrée»

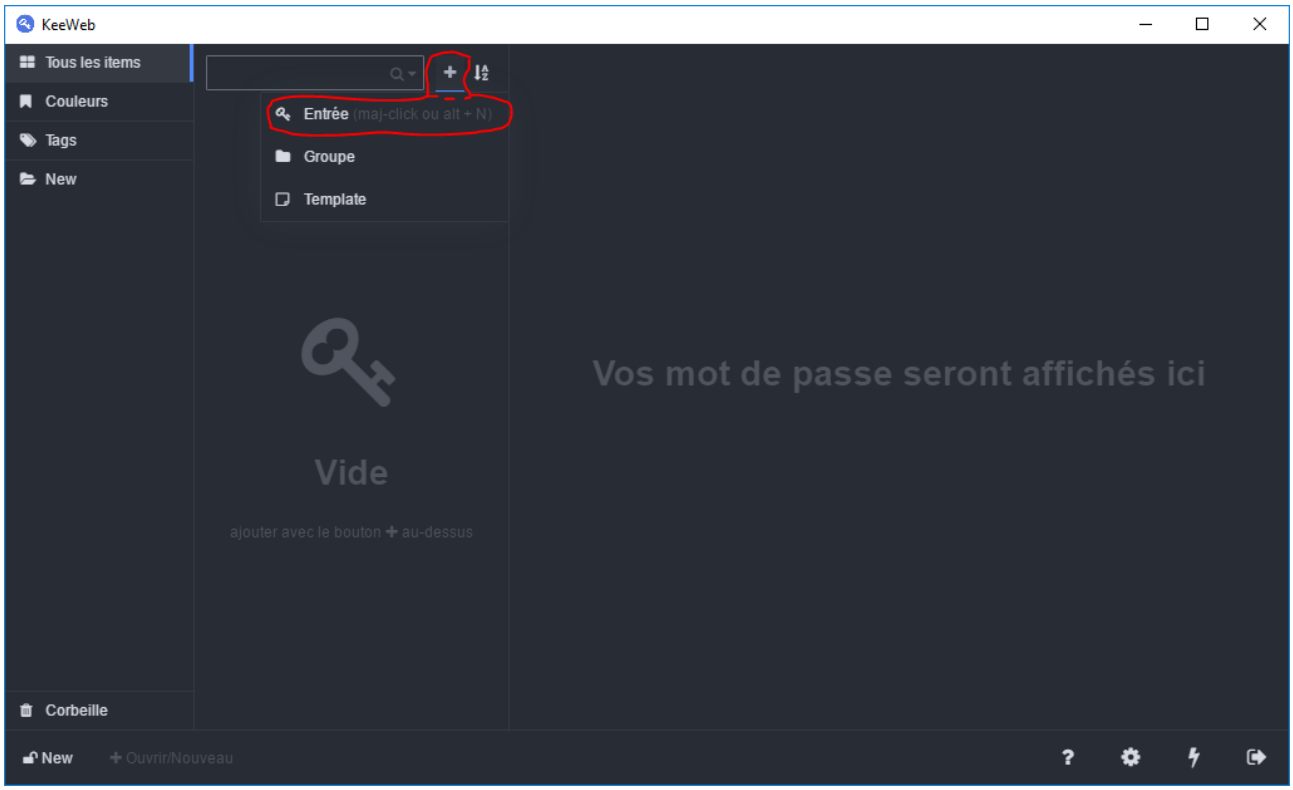

FIGURE 5. – Créer un nouveau mot de passe

Le troisième panneau des mots de passe se remplit alors, avec des champs qu'il ne reste plus qu'à compléter.

5. *Place à la pratique, utilisons ce fameux gestionnaire de mot de passe (KeeWeb)*

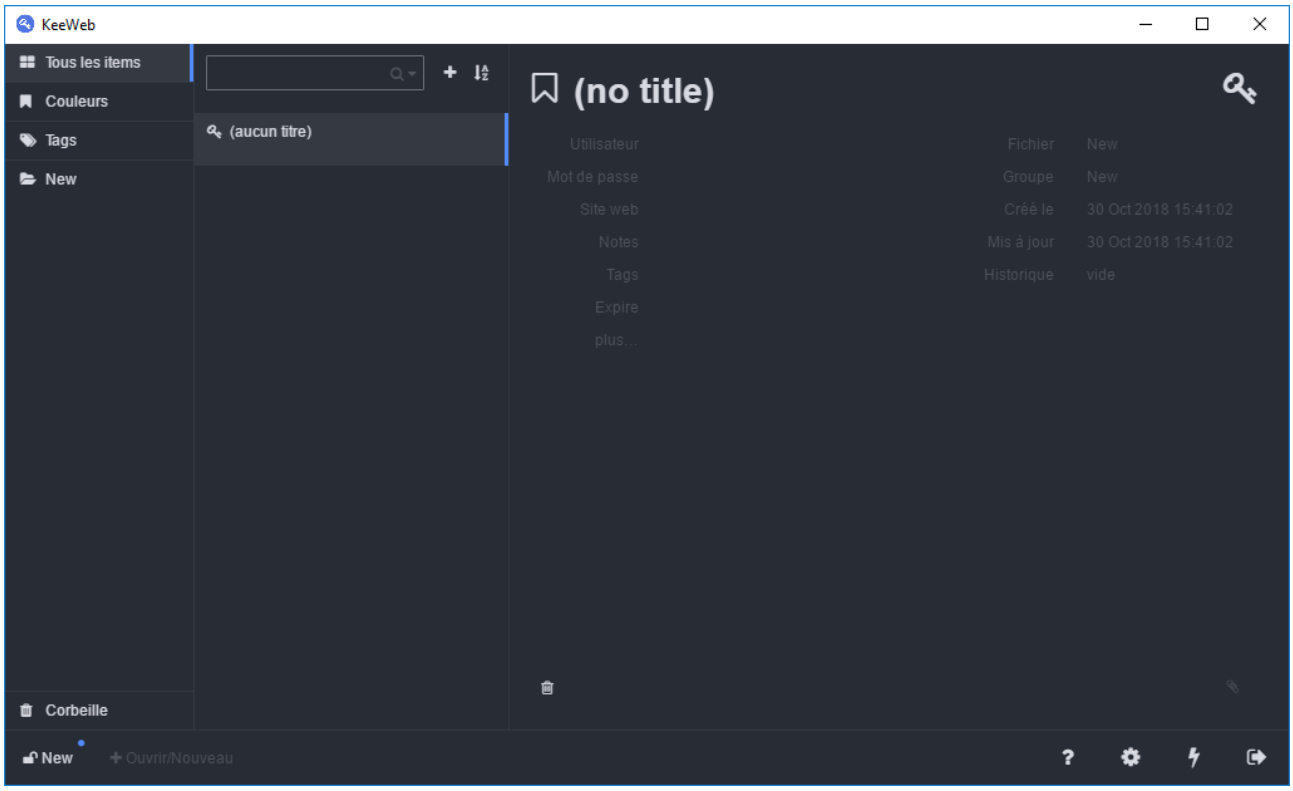

FIGURE 5. – Modèle de mot de passe

Pour l'exemple, je vous propose de créer un nouveau mot de passe pour un site imaginaire, pour lequel je devrais me connecter via le classique couple « courriel/mot de passe ». Je vais donc commencer par donner un nom à ce nouvel enregistrement, puis renseigné mon email comme étant le champ « utilisateur ». Enfin, il ne reste plus qu'à ajouter un mot de passe.

Et là intervient la magie !

Nous n'allons pas renseigner nous-même ce champ, mais demander au logiciel de nous générer un mot de passe complètement aléatoire selon certains critères. Par exemple, que le mot de passe fasse 16 caractères, contienne des majuscules, minuscules et un/des chiffre(s). On peut aussi lui demander de rajouter des caractères spéciaux. Pour faire tout cela, simplement cliquez sur le petit éclair à droite du champ «mot de passe».

5. *Place à la pratique, utilisons ce fameux gestionnaire de mot de passe (KeeWeb)*

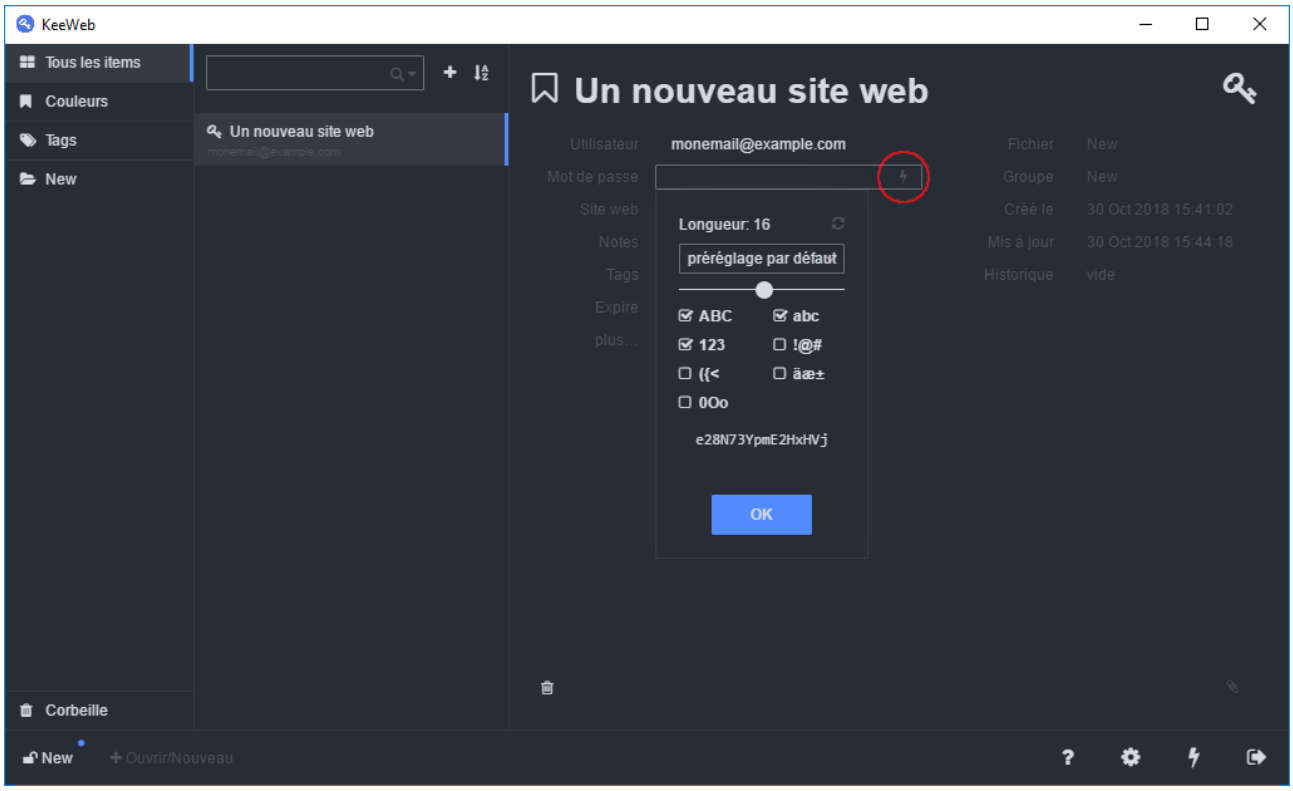

FIGURE 5. – Nouveau mot de passe

Une fois le mot de passe saisi, le champ devient «caché» et peut-être révélé d'un simple clic dessus. Il est aussi possible de rajouter des notes si vous voulez ajouter des informations à l'enregistrement.

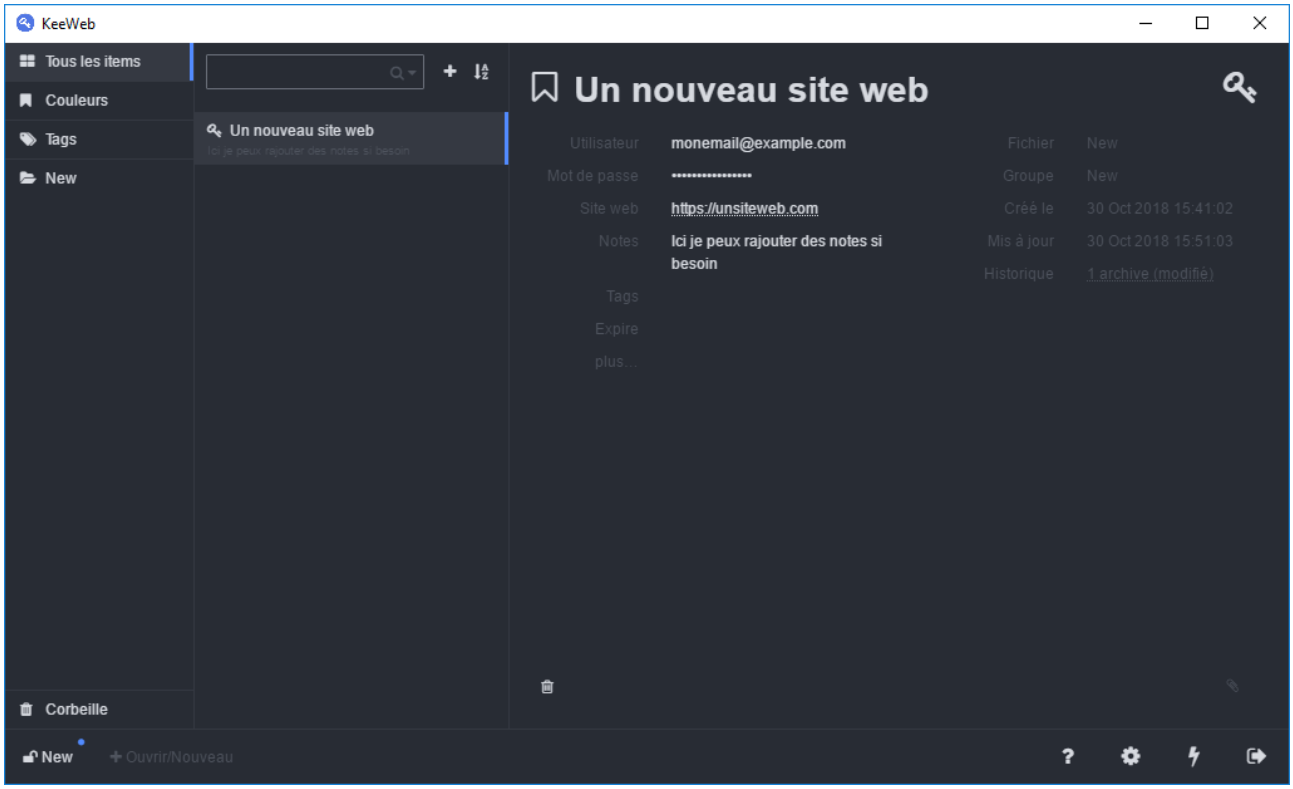

FIGURE 5. – Le mot de passe est créé !

Dernière étape, sauvegarder notre coffre-fort. Pour cela, cliquez sur l'onglet actuellement intitulé «New» tout en bas à gauche de l'application. L'écran suivant s'affiche alors.

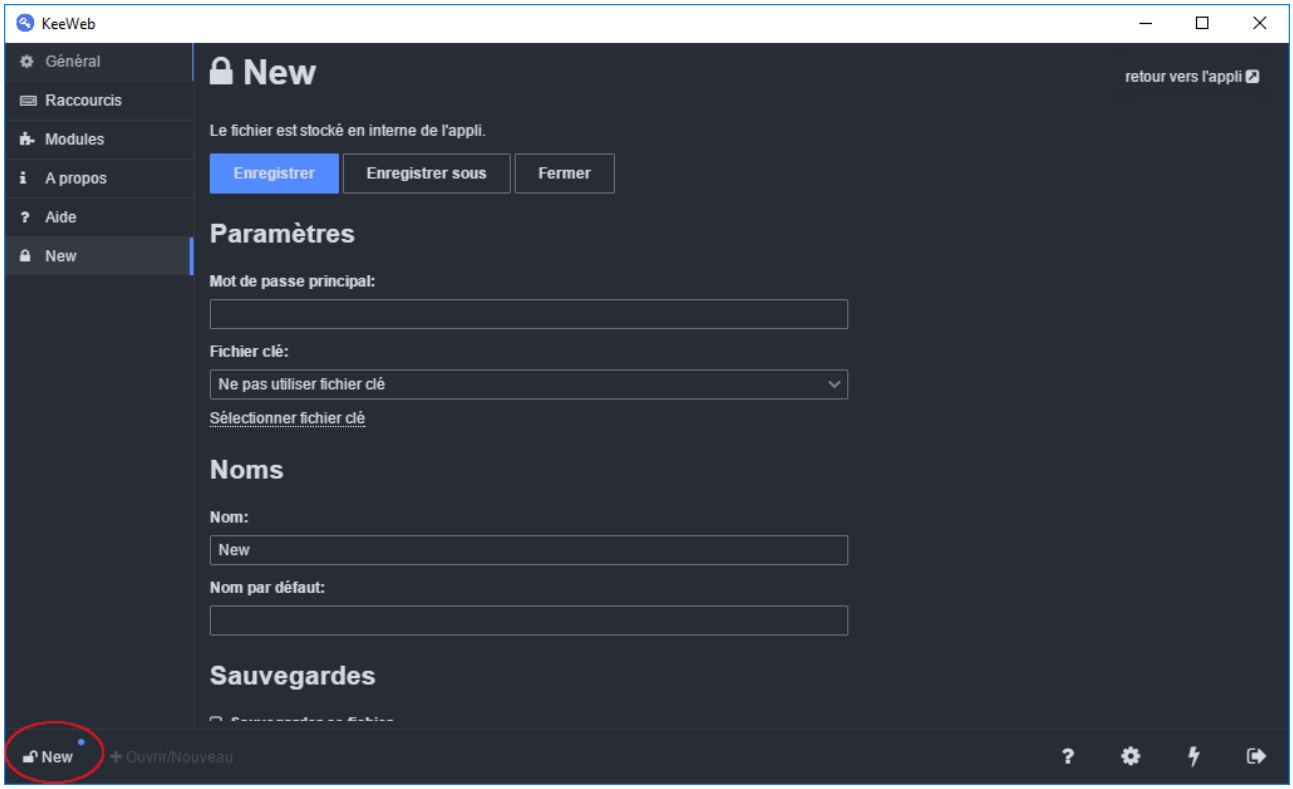

FIGURE 5. – Enregistrer le coffre-fort

Il vous faudra alors compléter deux champs. Le champ «Nom» qui permettra d'identifier le fichier (si jamais vous en utilisez plusieurs, lorsque vous êtes plusieurs à utiliser le même ordinateur par exemple) et le plus important, le champ «Mot de passe principal». Toute la sécurité de votre coffre-fort se situe ici.

C'est ce mot de passe que vous devez connaître par cœur et sera le seul à retenir !

Prenez donc 5 minutes pour penser à quelque chose qui vous convient, dont vous serez sûr de vous rappeler. Je vous rappelle qu'il faut que ce mot de passe soit fort, donc long (12 caractères et au-delà c'est un bon début) et difficile à deviner pour n'importe qui sauf vous ! Pas besoin de faire quelque chose d'incongru, une suite de mot suffisamment loufoque peut faire l'affaire, tant que vous arrivez à vous en souvenir.

Par exemple, la combinaison de mon coffre-fort ressemble à ceci : «LeChocolatFonduMauve». Il est facile à retenir une fois mémorisé car n'est pas incongru, mais pour autant ne sonne pas comme une évidence pour qu'un esprit extérieur puisse le deviner. On oublie donc les mots de passe à base de prénoms des enfants et de dates de naissance

Il ne reste plus qu'à cliquer sur «Enregistrer» et voilà, votre coffre-fort est en place. Dorénavant, la prochaine fois que vous ouvrirez le logiciel, ce dernier sélectionnera par défaut ce coffre-fort et vous demandera directement le mot de passe pour l'ouvrir.

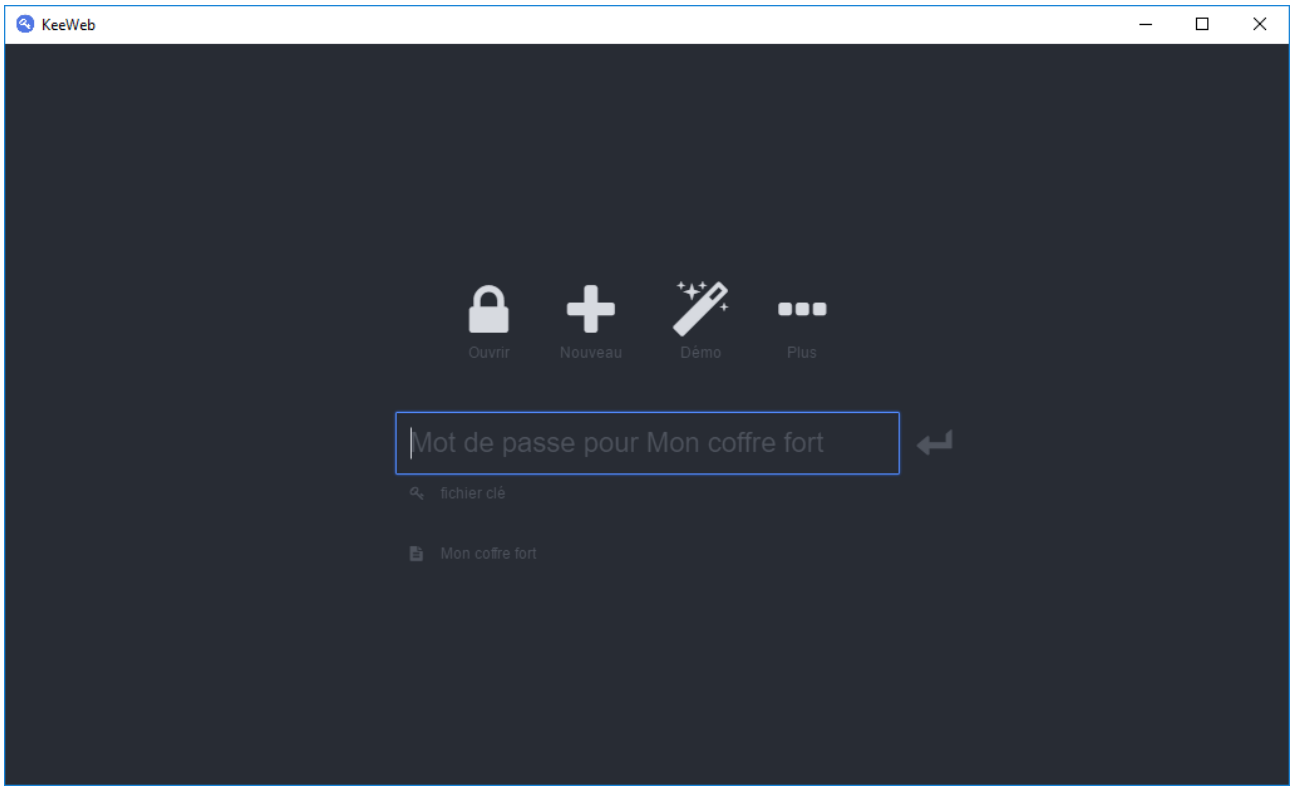

FIGURE 5. – Sésame ouvre-toi !

6. Synchroniser votre coffre-fort

Félicitations, vous avez mine de rien accompli un grand pas dans la sécurisation de votre vie privée en ligne !

Il me reste une chose à vous apprendre, qui est très simple : La synchronisation de votre coffre-fort.

Par synchronisation, je veux vous expliquer un mécanisme qui vous permettra de retrouver votre coffre-fort contenant tout vos mots de passe sur n'importe quel ordinateur ou smartphone connecté à internet. Pour cela, nous allons demander à KeeWeb d'envoyer et de garder à jour notre coffre-fort sur un service de stockage en ligne. Par défaut, 3 services grands public sont proposés : Dropbox, Google Drive et Microsoft OneDrive.

Une question émerge peut-être :

? Est-ce bien prudent de mettre tous mes mots de passe sur un service en ligne qui peut-être sujet à des failles de sécurité ?

Et c'est une excellente question. Le fichier, représentant votre coffre-fort, qui va se synchroniser sur les services en ligne est dit "chiffré". Cela signifie que son contenu est inaccessible. Tout comme si vous récupériez un coffre-fort sans son code, vous ne pourriez l'ouvrir.

Contenu masqué n°1

Pour réaliser cette synchronisation, il vous faudra donc un compte sur l'un de ces trois services. Ensuite, lorsque vous allez ouvrir KeeWeb, ouvrez votre coffre-fort puis sélectionner son onglet en bas à gauche. Ensuite, cliquez sur le bouton «Enregistrer sous». Des options apparaissent alors, il ne vous reste plus qu'à sélectionner celle que vous souhaitez puis suivre les instructions de connexion au compte utilisé.

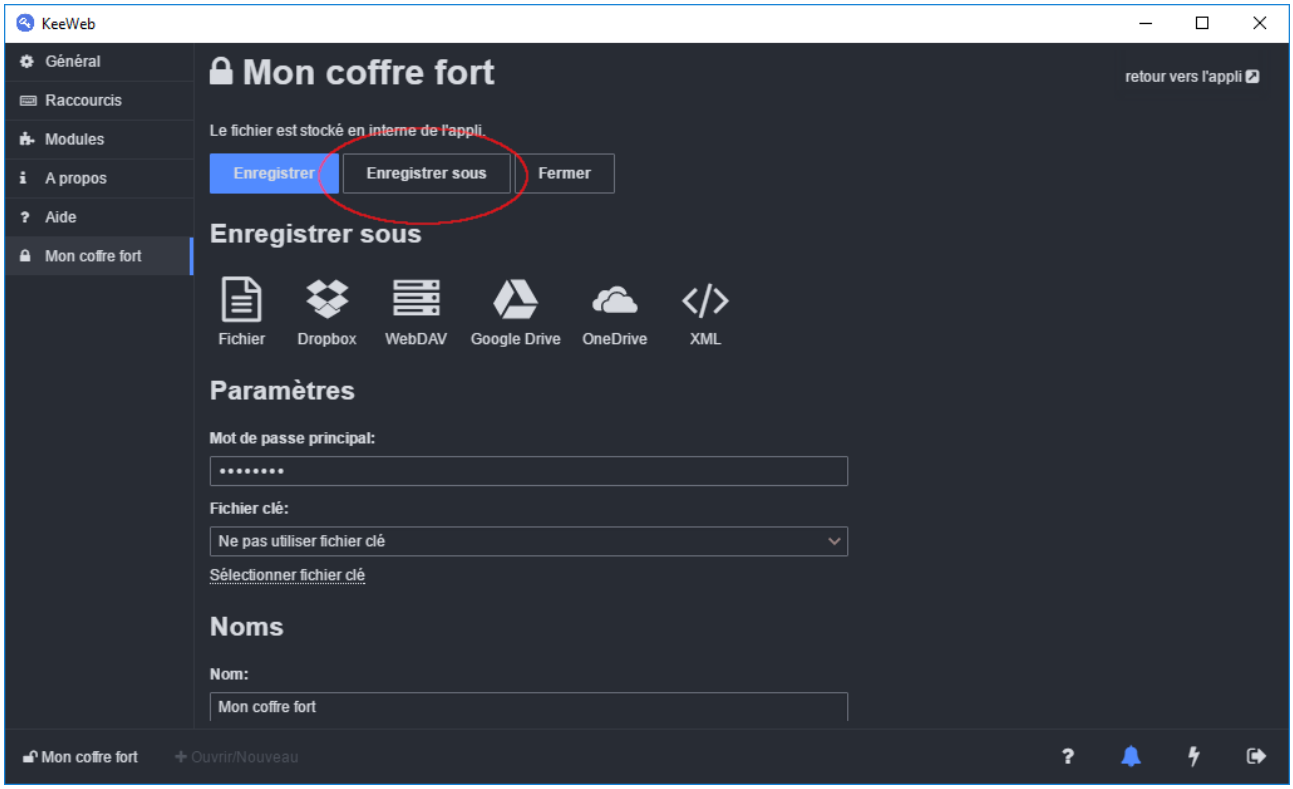

FIGURE 6. – Synchroniser votre coffre-fort

Dorénavant, à chaque fois que vous allez créer ou éditer un mot de passe, KeeWeb se chargera automatiquement de faire une synchronisation avec la version distante, afin que vous puissiez utiliser votre coffre-fort partout, en toute circonstance.

7. Quelques astuces pour rendre l'utilisation moins fastidieuse

Pour conclure ce tutoriel, je souhaite vous partager quelques astuces pour rendre l'utilisation d'un gestionnaire de mot de passe plus agréable et productive au quotidien.

7.1. Changer les comptes petits à petits

Utiliser un gestionnaire de mot de passe, c'est une gymnastique, une routine, qui peut prendre du temps. Une fois mise en place cependant, les bénéfices se font sentir et aucune contrainte n'apparait.

Une approche radicale de la sécurité serait de dire «Changez dès aujourd'hui vos mots de passe pour en mettre un fort et unique partout». Je vais toutefois vous proposer une approche plus modérée et plus compatible avec le quotidien.

Ce que je vous propose, c'est que la prochaine fois que vous vous connecter à un service que vous utilisez déjà, avec peut-être un mot de passe que vous utilisez partout, vous alliez dans les options de votre profil pour ce site pour aller changer votre mot de passe. Et c'est tout !

L'idée est de ne pas faire un inventaire immédiat de tout les sites et services que vous utilisez pour passer une demi-journée à les mettre à jour, mais plutôt d'avoir une approche progressive, en faisant un site à la fois, une fois de temps en temps. Ainsi, a priori les sites que vous consultez le plus et qui donc vous sont les plus sensibles, seront sécurisés rapidement. Les autres viendront ensuite, petit à petit.

7.2. Demander au navigateur de travailler pour vous

> ! Ce conseil ne s'applique que sur un ordinateur personnel, ne le faites pas sur un ordinateur public !

Afin de diminuer un peu la charge de travail, tous les navigateurs internet modernes et à jour propose une fonctionnalité de «mémorisation» des mots de passe. Pourquoi ne pas l'utiliser en parallèle du gestionnaire de mots de passe. Ce dernier crée des mots de passe compliqués et les sauvegardes pour vous pour les rendre accessibles partout, puis le navigateur se charge de s'en souvenir localement pour vous éviter d'avoir à les saisir sans arrêt.

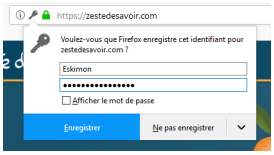

FIGURE 7. – Exemple pour Firefox, se souvenir de mon mot de passe

7.3. Utiliser la touche de remplissage automatique

KeeWeb possède quelques raccourcis clavier pour vous rendre la vie plus facile. Je trouve l'un d'entre eux particulièrement utile : La complétion automatique. Grâce à cette fonction, KeeWeb se chargera de compléter intelligemment les champs login / mot de passe du service auquel vous souhaiter accéder.

Pour l'utiliser c'est assez simple. Tout d'abord, allez sur la page de connexion du service/site web auquel vous souhaitez vous connecter. Ensuite, ouvrez KeeWeb et sélectionner la fiche du

mot de passe concerné. Enfin, faites un appui sur les touches Ctrl + T (restez appuyé sur la touche Ctrl puis appuyer sur T). Si tout se passe bien et que KeeWeb arrive à reconnaître les champs du formulaire, ce dernier va alors automagiquement se compléter tout seul.

Voici la liste de tout les raccourcis clavier possibles :

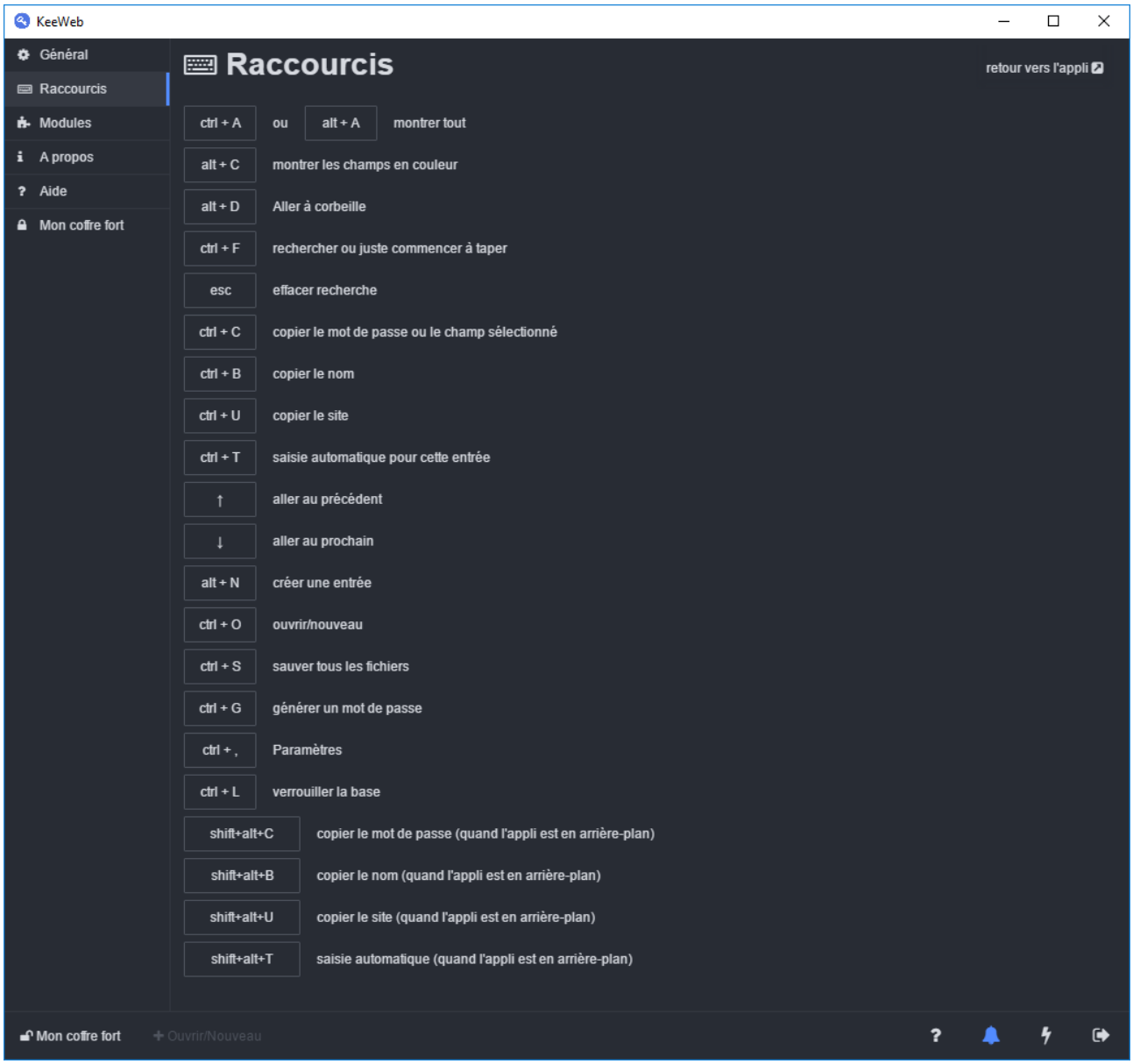

FIGURE 7. – Raccourcis clavier

7.4. Application mobile suggérée

Enfin, un dernier conseil que je vous suggère est d'utiliser aussi un gestionnaire de mots de passe sur votre mobile. En le synchronisant, vous pourrez retrouver vos mots de passe pour les sites web, mais aussi ajouter ceux pour vos applications.

Sur Android, je vous recommande Keepass2Android (lien Google Play). L'interface n'est pas des plus élégantes, mais elle fait le travail.

N'utilisant pas iOs, je ne suis pas en mesure de faire une suggestion éclairée. Apparemment l'application MiniKeePass (lien iTunes) semble bonne.

Ces deux applications sont bien entendues 100% compatibles avec les coffres-fort générés par KeeWeb. En effet, toutes ces applications utilisent l'écosystème de gestion de mots de passe «KeePass» permettant des interactions entre elles.

8. Conclusion

Voilà, ce tutoriel touche à sa fin. J'espère qu'il aura su vous intéresser sans vous égarer dans des termes ou des concepts superflus. L'utilisation d'un gestionnaire de mot de passe au quotidien n'est vraiment pas compliquée et demande juste de s'y habituer. La récompense d'une sécurité vraiment accrue sur vos services en ligne est quant à elle bien réelle !

Profitons de ces quelques lignes pour glisser des remerciements à tous ceux qui ont pu participer à la vie de ce tuto en le relisant et en corrigeant mes fautes, ainsi qu'un coucou à @qwerty pour la validation.

Contenu masqué

Contenu masqué n°1

Les petits malins me diront qu'un coffre-fort peut-être percé ou dynamité pour être ouvert. Et c'est aussi le cas pour le chiffrement numérique de ce coffre-fort numérique. Toutefois, les *algorithmes* utilisés pour réaliser cette opération sont tellement perfectionnés que cette opération de dynamitage numérique (appelé *brute force*) n'est pas réalisable en «temps humain». C'est-à-dire qu'elle n'est pas réalisable avant que la donnée ne soit devenue obsolète ou alors protégé par un meilleur moyen. Retourner au texte.