TP Gestion de mot de passe

Réalisé par CEVIK Meryem

Travail à faire

a. Sensibilisation

Réaliser une plaquette permettant de sensibiliser les utilisateurs au sujet de leur mot de passe.

b. Statistique

Réaliser un tableau de statistique (au moins 20 mots de passe) montrant la fragilité de ceux-ci

c. Gestionnaire de mot de passe

Identifier un gestionnaire de mot de passe pouvant être utilisé au sein de votre entreprise et rédiger la procédure d'installation et d'utilisation

a. Sensibilisation

LES MOTS DE PASSE - PROTEGEZ VOS INFORMATIONS CONFIDENTIELLES

Un mot de passe sécurisé est la première étape pour protéger vos informations confidentielles en ligne. Qu'il s'agisse de votre adresse e-mail, de votre compte bancaire ou de votre profil sur les réseaux sociaux, un mot de passe fort est essentiel pour empêcher les pirates informatiques d'accéder à vos informations. Voici une liste de bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

UTILISEZ UN MOT DE PASSE DIFFÉRENTS POUR CHAQUE COMPTE

Il est essentiel d'utiliser des mots de passe différents pour chaque compte en ligne que vous possédez. En cas de perte ou de vol d'un mot de passe, le service concerné serait le seul vulnérable, sans affecter les autres comptes que vous possédez. En revanche, si vous utilisez le même mot de passe pour plusieurs services, tous les services compromis seraient alors exposés à des risques de piratage.

UTILISEZ UN MOT DE PASSE SUFFISAMMENT COMPLIQUE ET LONG

Il est important d'utiliser des mots de passe suffisamment longs et complexes pour renforcer leur sécurité. Un mot de passe court et simple peut être facilement deviné par un pirate informatique, ce qui pourrait mettre en danger vos informations personnelles et confidentielles. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 16 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Pour protéger vos comptes en ligne, il est crucial d'utiliser un mot de passe impossible à deviner. Les pirates informatiques utilisent souvent des techniques pour essayer de « deviner » votre mot de passe. Il est donc important d'éviter d'utiliser des informations personnelles dans votre mot de passe, telles que votre date de naissance, votre nom ou celui de votre animal de compagnie, ou encore votre groupe de musique préféré. Les pirates informatiques utilisent des outils automatisés pour tester des milliers de combinaisons de mots de passe, et plus votre mot de passe est complexe et unique, plus il sera difficile à deviner.

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Un gestionnaire de mots de passe est un outil qui vous aide à stocker tous vos mots de passe de manière sécurisée. Au lieu de devoir vous souvenir de chaque mot de passe que vous avez créé pour chacun de vos comptes en ligne, vous pouvez les stocker dans le gestionnaire de mots de passe, qui vous permettra d'y accéder facilement quand vous en avez besoin.

KEEPASS

Ce logiciel libre, gratuit et en français, certifié par l'**ANSSI**, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

https ://keepass.info

Le gestionnaire de mots de passe chiffre également vos informations de connexion pour vous assurer qu'elles ne seront pas interceptées par des pirates informatiques. Il est très important de ne pas stocker vos mots de passe sur des post-its, des notes sur votre téléphone ou sur votre ordinateur car cela peut rendre vos informations vulnérables aux attaques de pirates informatiques. En utilisant un gestionnaire de mots de passe, vous pouvez vous assurer que vos informations de connexion sont stockées en toute sécurité.

CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Lorsque vous soupçonnez que quelqu'un d'autre a peut-être accédé à votre compte, il est important de le changer immédiatement. Cela peut se produire si vous avez partagé votre mot de passe avec quelqu'un, si vous avez cliqué sur un lien suspect ou si vous avez remarqué une activité inhabituelle sur votre compte. En changeant votre mot de passe régulièrement, vous vous assurez que personne ne peut accéder à votre compte sans autorisation.

NE PARTAGEZ JAMAIS VOTRE MOT DE PASSE A QUI QUE CE SOIT

Il est essentiel de ne jamais partager votre mot de passe avec quiconque. Cela inclut vos amis, votre famille, vos collègues de travail et même les personnes prétendant être du support technique de votre entreprise ou service en ligne. Le partage de mots de passe peut entraîner des conséquences graves, comme la perte de contrôle sur vos informations personnelles, financières ou professionnelles. De plus, si vous partagez votre mot de passe avec quelqu'un d'autre et que cette personne commet une infraction en utilisant votre compte, vous pourriez être tenu pour responsable. Il est important de garder votre mot de passe personnel et confidentiel.

N'UTILISEZ PAS VOS MOTS DE PASSE SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

ACTIVEZ L'AUTHENTIFICATION A DEUX FACTEURS LORSQUE C'EST POSSIBLE

Il est important de prendre des mesures de sécurité pour protéger vos comptes en ligne. Une méthode efficace est d'activer l'authentification à deux facteurs (2FA). De nombreux services en ligne proposent cette fonctionnalité qui ajoute une couche de sécurité supplémentaire à votre compte.
Lorsque vous activez l'authentification à deux facteurs, vous ajoutez une couche de sécurité supplémentaire à votre compte. En plus de votre mot de passe, vous devrez également fournir une autre information pour vous connecter, comme un code de sécurité unique envoyé à votre téléphone portable ou une empreinte digitale. Cela rend beaucoup plus difficile pour les pirates informatiques d'accéder à votre compte, même s'ils ont réussi à voler votre mot de passe. Donc, chaque fois que c'est possible, n'hésitez pas à activer l'authentification à deux facteurs pour renforcer la sécurité de vos comptes en ligne.

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Gmail, Yahoo Mail…
- Facebook, Instagram, LinkedIn, Twitter…
- Skype, WhatsApp…
- Amazon, eBay, Paypal…
- Apple iCloud, Dropbox, Google Drive, OneDrive…

CHANGEZ LES MOTS DE PASSE PAR DÉFAUT DES DIFFÉRENTS SERVICES

Lorsque vous créez un compte sur un service en ligne, il est souvent accompagné d'un mot de passe par défaut générique, facile à deviner pour les pirates informatiques. Par conséquent, il est impératif de changer le mot de passe par défaut dès que possible, afin d'augmenter la sécurité de votre compte. Les pirates informatiques utilisent des outils automatisés pour essayer de se connecter à des comptes en ligne avec des mots de passe par défaut, il est donc important d'utiliser un mot de passe fort et unique

pour chaque compte. N'oubliez pas de changer régulièrement vos mots de passe pour garantir la sécurité de vos comptes en ligne.

CHOISISSEZ UN MOT DE PASSE PARTICULIÈREMENT RESISTANT POUR VOTRE MESSAGERIE

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle. Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger.

b. Statistique

Mot de passe	Complexité	Longueur	Types de caractères utilisés	Temps pour le craquer
123456	Faible	6	Chiffres	Moins d'une seconde
123456789	Moyenne	9	Chiffres	Moins de 1 minute
azertyuiop	Faible	10	Lettres	Moins d'une seconde
password	Faible	8	Lettres	Moins d'une seconde
12345678	Moyenne	8	Chiffres	Moins de 1 minute
qwertyuiop	Faible	10	Lettres	Moins d'une seconde
1234567	Faible	7	Chiffres	Moins d'une seconde
1234567890	Moyenne	10	Chiffres	Moins de 1 minute
123456789	Moyenne	10	Chiffres	Moins de 1 minute
azerty123	Moyenne	8	Lettres, chiffres	Moins de 1 minute
0	Faible	6	Chiffres	Moins d'une seconde
soleil	Faible	6	Lettres	Moins d'une seconde
france	Faible	6	Lettres	Moins d'une seconde
iloveyou	Faible	8	Lettres	Moins d'une seconde
abcdefgh	Faible	8	Lettres	Moins d'une seconde
123123	Faible	6	Chiffres	Moins d'une seconde
letmein	Faible	7	Lettres	Moins d'une seconde
111111	Faible	6	Chiffres	Moins d'une seconde
admin	Faible	5	Lettres	Moins d'une seconde
mdpasse$	Forte	8	Lettres, chiffres, caractères spéciaux	Moins de 57 jours

Ce tableau montre que la plupart des mots de passe sont faibles en termes de complexité et sont constitués soit de chiffres, soit de lettres.

Les mots de passe qui contiennent une combinaison de lettres et de chiffres sont généralement plus complexes et plus sûrs que les mots de passe qui ne contiennent que des lettres ou des chiffres. Seul le dernier mot de passe dans la liste prendrait plus de temps pour être craqué, car il est plus long et plus complexe.

En général, il est recommandé d'utiliser des mots de passe qui sont complexes, longs et qui contiennent un mélange de chiffres, de lettres et de caractères spéciaux pour une meilleure sécurité.

c. Gestionnaire de mot de passe

Introduction :

Un gestionnaire de mots de passe est un type de logiciel qui permet à un utilisateur de centraliser l'ensemble de ses identifiants et mots de passe dans une base de données accessible par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir.

J'ai choisi le produit KeePass 2.53 qui est un gestionnaire de mot de passe certifiée par l'ANSSI.

Le logiciel open source KeePass est un coffre-fort de mots de passe qui permet aux utilisateurs d'enregistrer sur un même support, c'est-à-dire sur un seul un fichier entièrement protégé, leurs différents mots de passe utilisés sur Internet.

Nous allons voir comment l'installer et l'utiliser.

Figure 1 : Logo de Keepass

Installation :

Keepass est téléchargeable gratuitement sur le site officiel : https://keepass.info/.

Figure 2 : Téléchargé l'outil pour windows

Création de la base de données :

Tout d'abord, il faut créer une base de données. La base de données peut être sécurisée par l'utilisation d'un mot de passe principal ou/et d'un fichier clé.

Il faut bien créer un mot de passe fort, pour s'aider la barre 'Estimated quality' permet de vérifier la complexité du mot de passe.

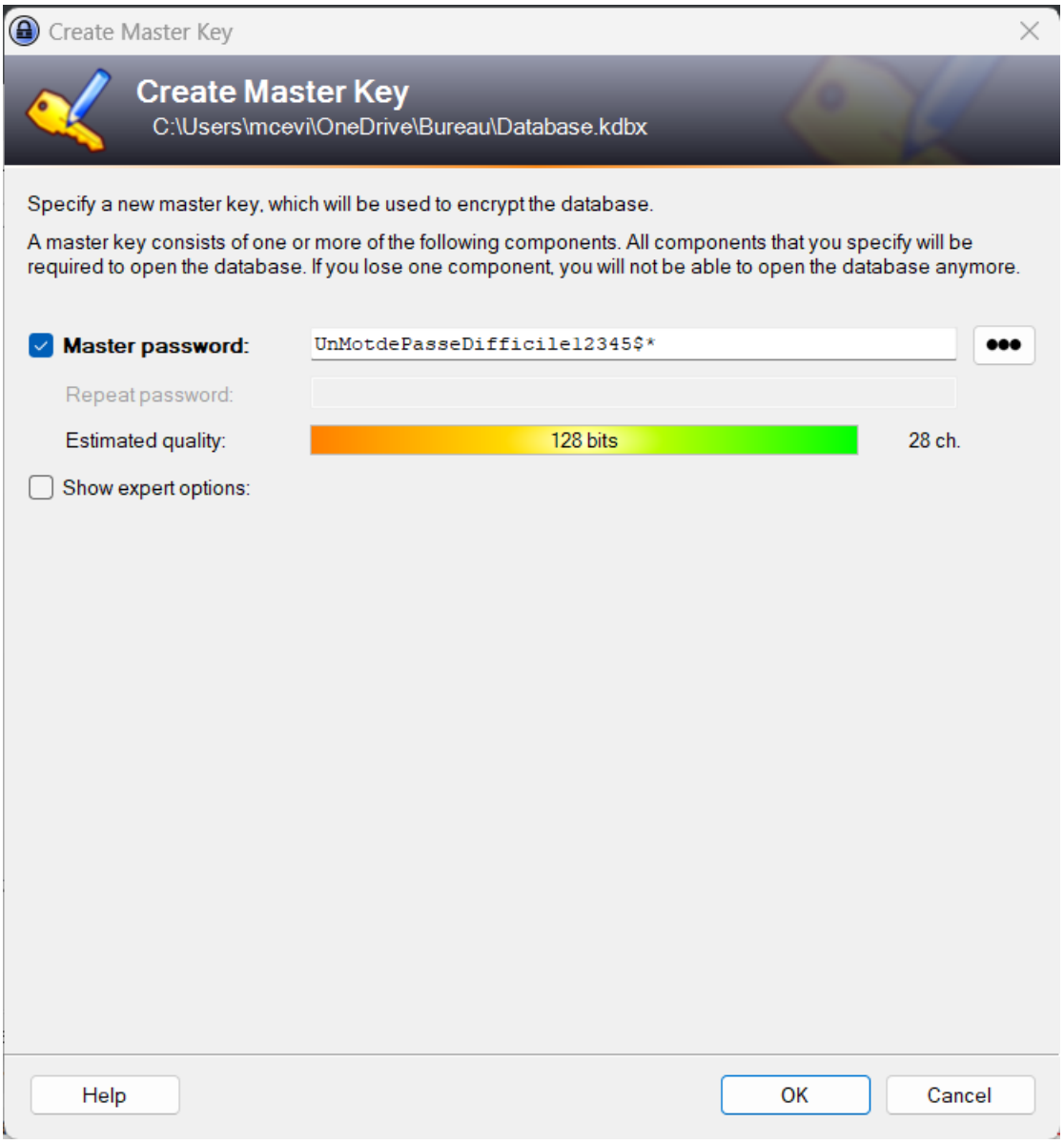


Figure 3 : Création de la base de données

Une fois la base de données créée, on a l'interface d'utilisation:

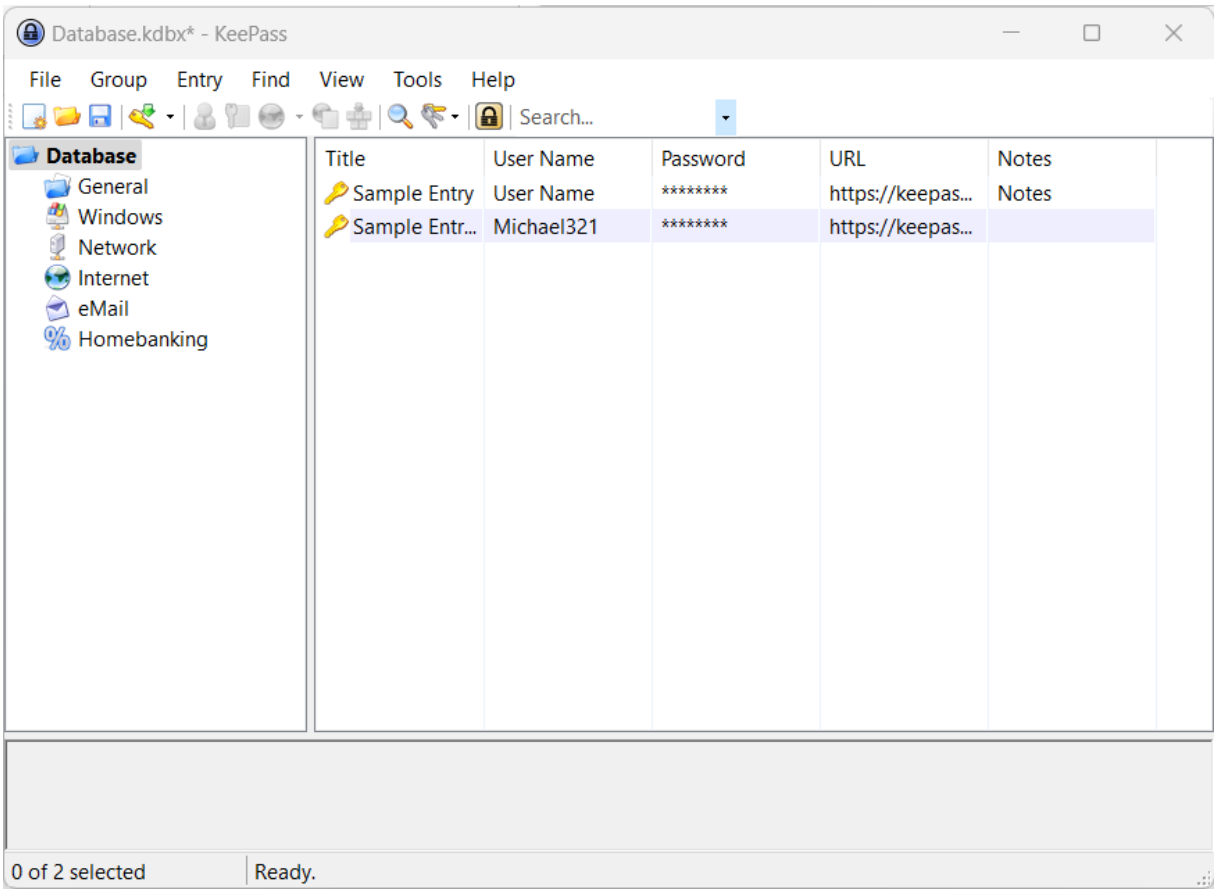


Figure 4 : Interface d'utilisation de Keepass

Création de mot de passe :

Pour une utilisation simplifiée, on doit créer des groupes. Pour cela on sélectionne *Group > Add Group*.

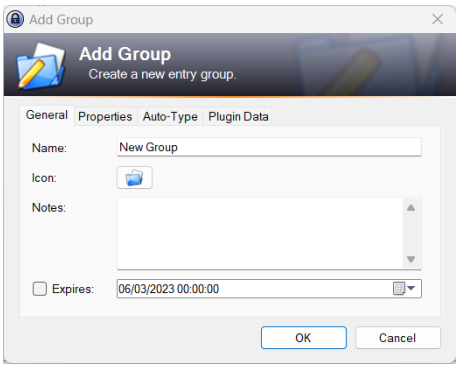


Figure 5 : Ajout de groupe

Une fois le groupe créé, on ajoute ensuite une nouvelle entrée (Menu Entry -> Add entry). Par exemple, nous allons ajouter une entrée pour un compte sur un site web ici pour Amazon.

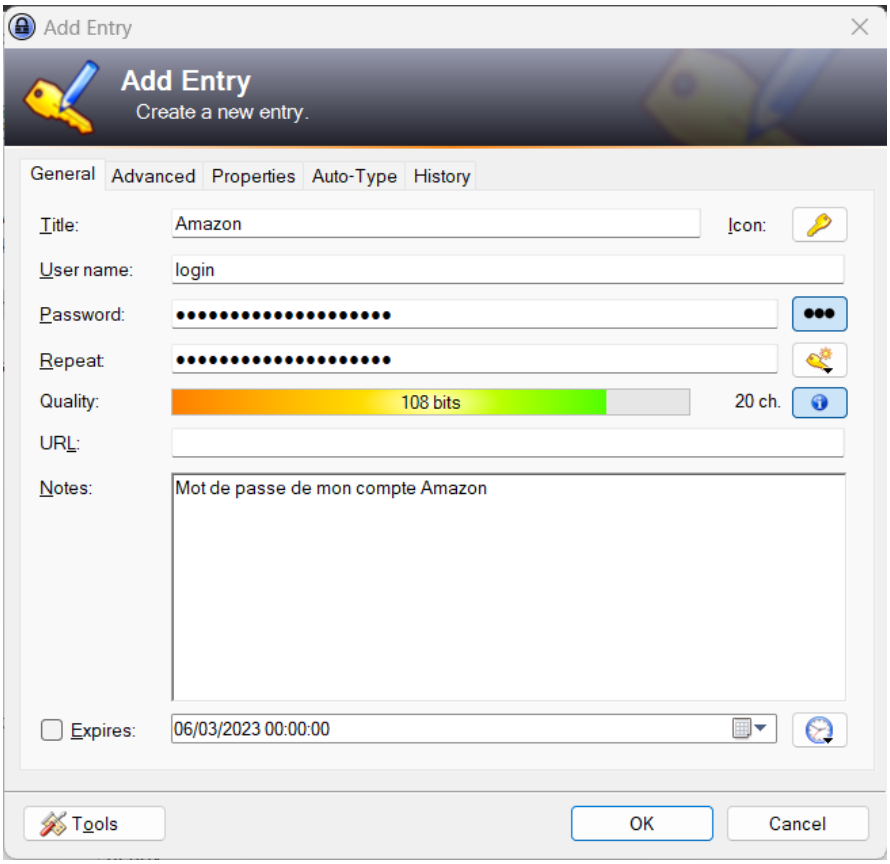


Figure 6 : Ajout d'une nouvelle entrée

Pour récupérer ce mot de passe :

- On fait une clique droite sur l'entrée puis on sélectionne *'Copy Password'*.

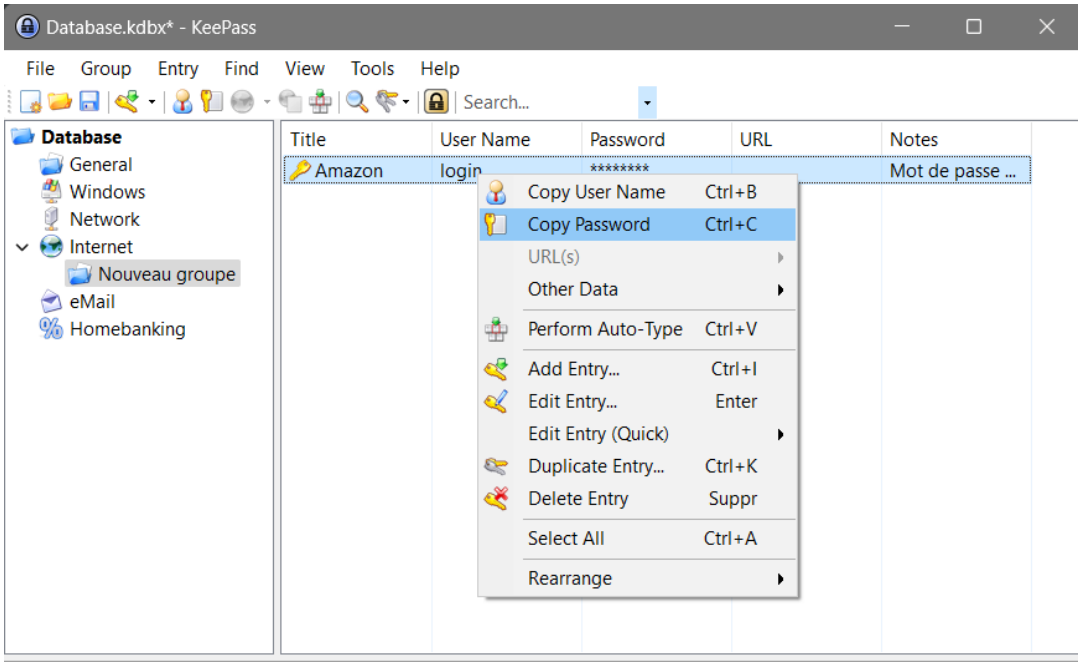


Figure 7 : Récupérer son mot de passe 1

- Ou bien on clique sur l'entrée puis on clique sur les points de suspension pour voir le mot de passe au clair.

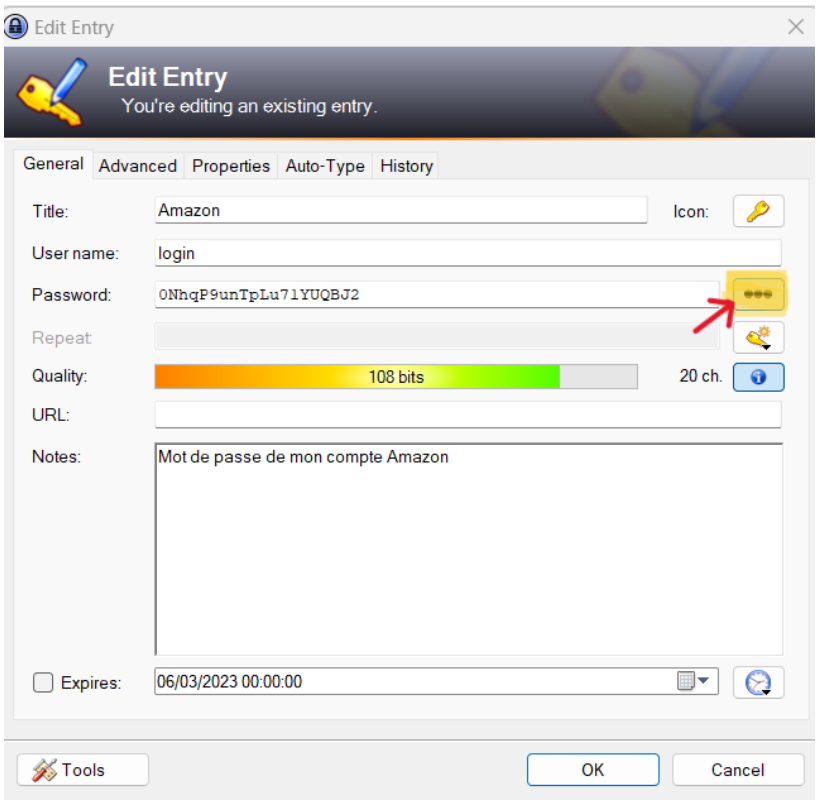


Figure 8 : Récupérer son mot de passe 2

Concernant le choix du mot de passe, c'est plus sécurisé de générer un mot de passe aléatoire. Le générateur permet ainsi de définir les caractères à utiliser ainsi que la longueur du mot de passe (le plus long possible puisqu'il n'est plus nécessaire de s'en souvenir).

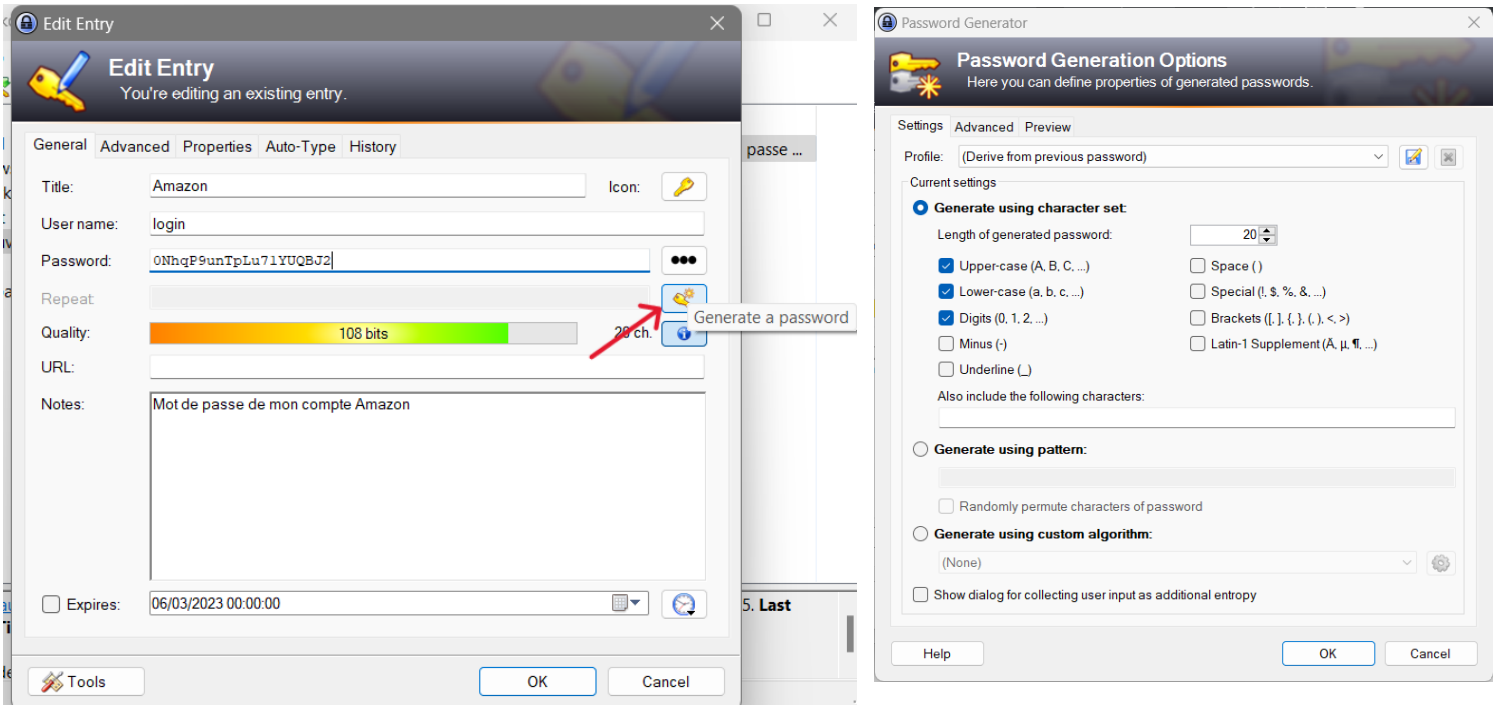
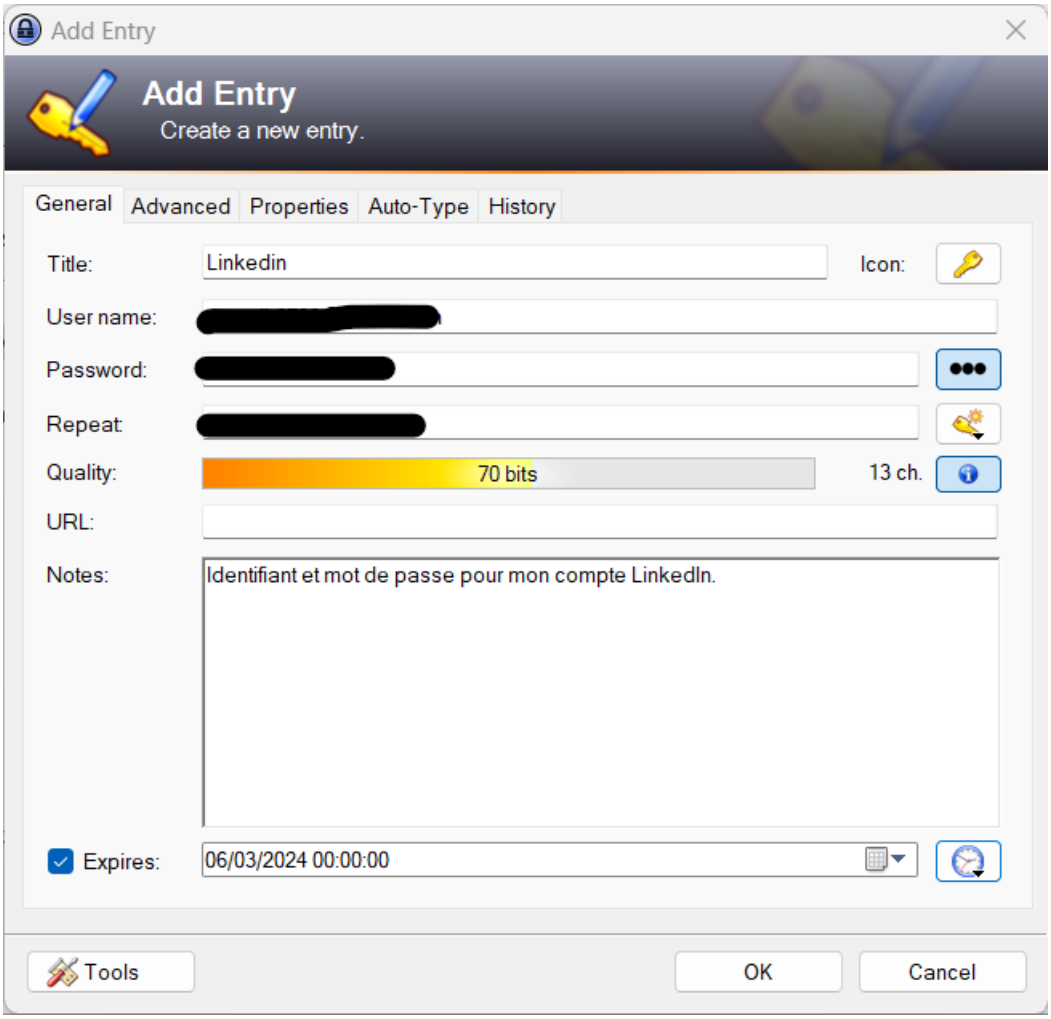


Figure 9 : Générateur de mot de passe

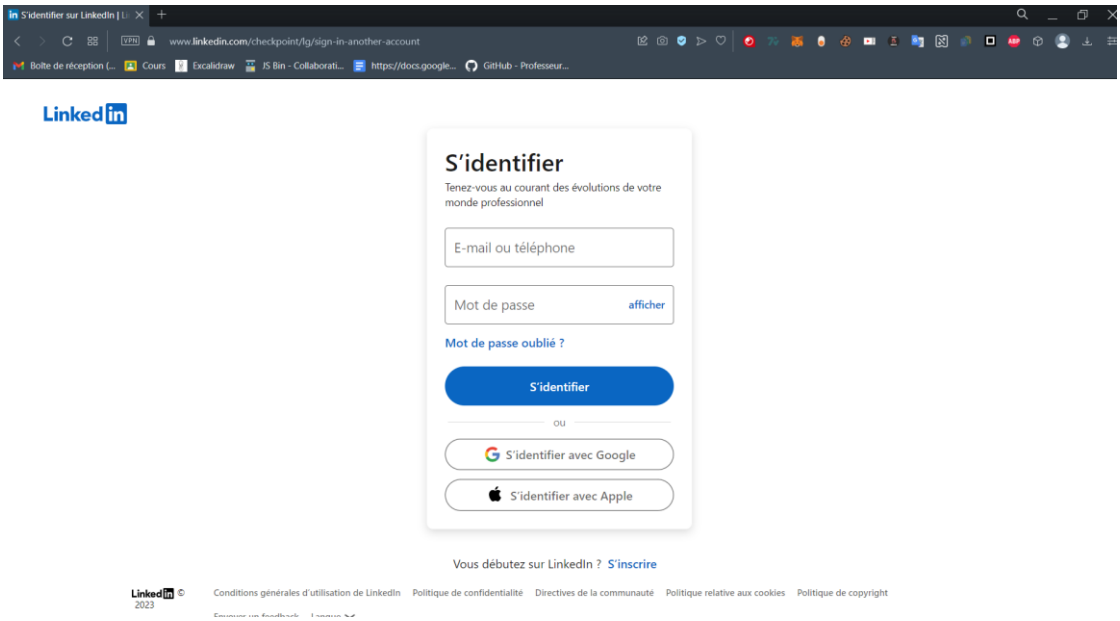
Authentification

KeePass gère l'authentification sur les sites, il auto-complète la partie login et mot de passe. On va essayer sur le site web linkedin.com.

On crée une nouvelle entrée comme on vient de faire et en renseigne notre identifiant et mot de passe pour se connecter à notre compte LinkedIn.



Maintenant, il faut aller sur la page de connexion du site et copier l'url.



On colle l'adresse de la page dans la partie URL de Keepass :

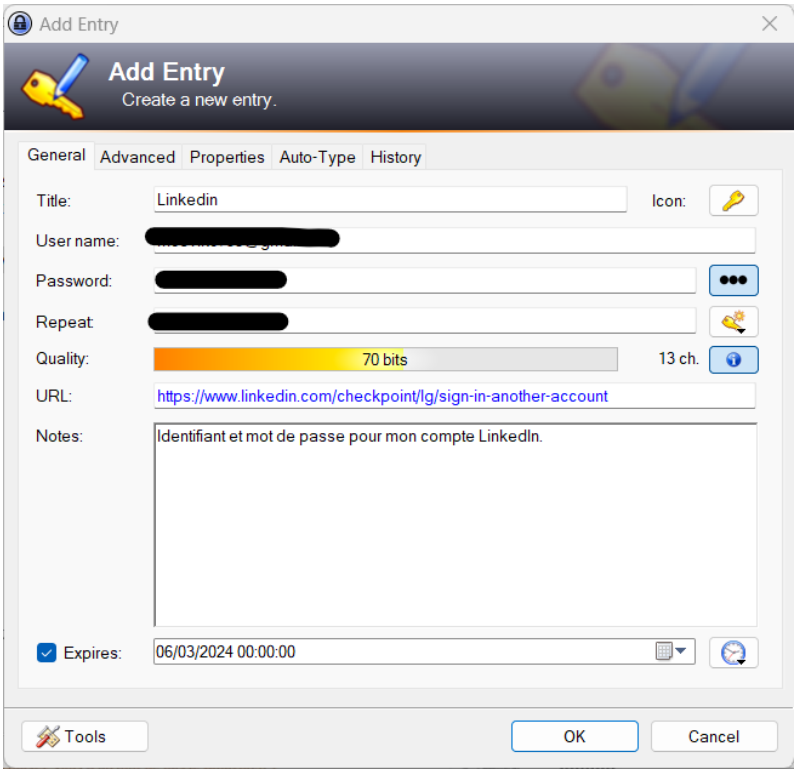


Figure 10 : Ajout URL

Puis on clique sur Ok pour enregistrer les modifications. Puis on fait une clique droite sur l'entrée puis on sélectionne *URL(s) > open*.

Un onglet s'ouvre qui correspond à l'url renseigné. Il nous reste juste la partie auto-complétée qu'on l'obtient en cliquant sur *'Perform Auto-type'*.

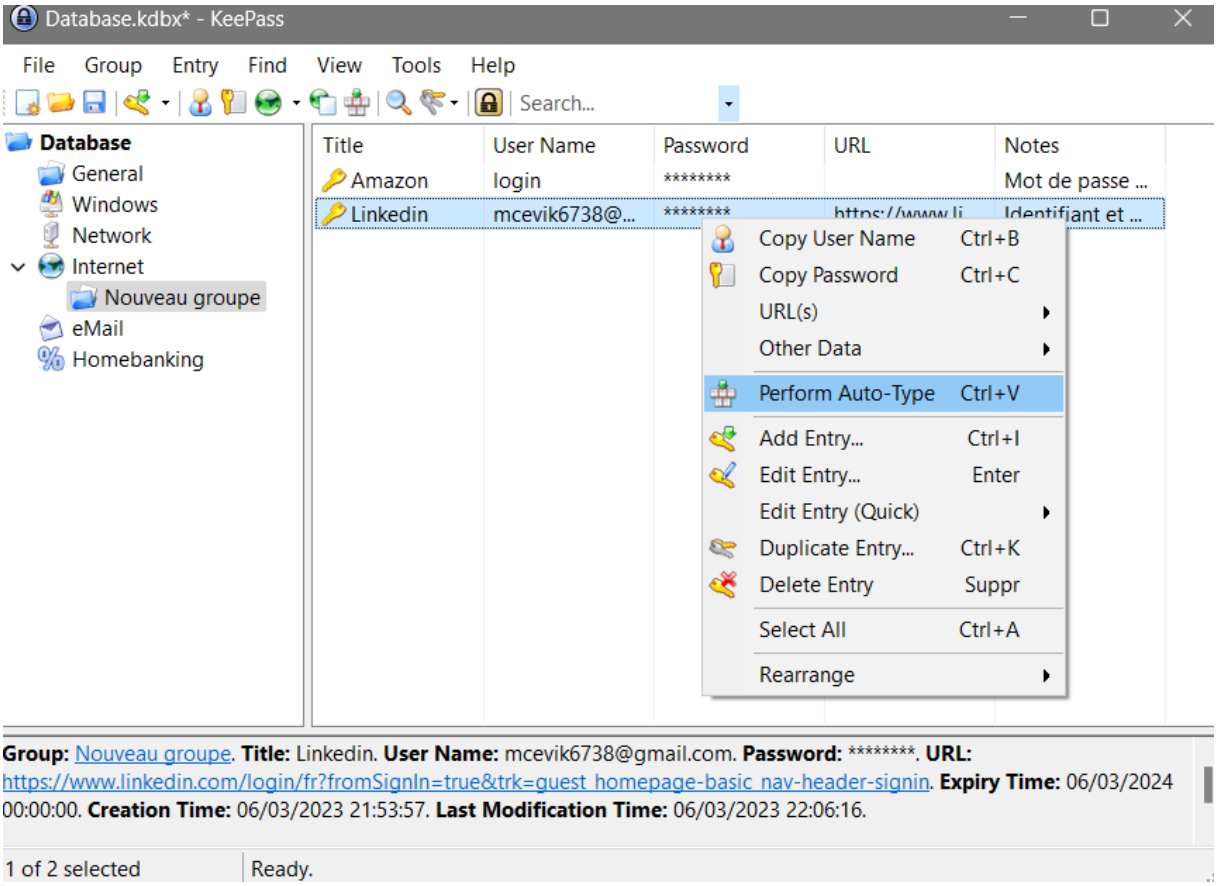


Figure 11 : Sélection Auto-type dans Keepass

Et voilà le formulaire s'auto-complète avec l'identifiant et le mot de passe.

Note : Sur une application hors ligne, KeePass ne permet pas de fonction d'auto-complétions, il faut renseigner les informations d'authentification manuellement.