KeePass, gestionnaire de mots de passe sécurisé

Avec l'utilisation croissante de mots de passe complexes et régulièrement renouvelés pour protéger nos données et comptes en ligne, la gestion des mots de passe peut s'avérer très complexe. C'est pourquoi il est recommandé d'utiliser un gestionnaire de mots de passe pour nous aider à gérer cette tâche. Cette fiche vous explique comment utiliser KeePass (ou l'une de ses variantes recensées sur https://keepass.info/download.html).

Qu'est-ce que KeePass ?

KeePass est un logiciel open source gratuit conçu pour stocker et gérer les mots de passe. Il est compatible avec tous les systèmes d'exploitation et tous les appareils (ordinateur sous Windows, Linux ou MacOS). Cette application est certifiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

KeePass a aussi des variantes pour iOS et Android. Il suffit de télécharger l'application sur Apple Store ou Play Store.

Il vous permet de conserver un seul fichier chiffré contenant une liste complète de mots de passe. Ce fichier peut être ensuite ouvert et modifié à partir d'un mot de passe principal. Cela signifie que vous n'aurez plus besoin de mémoriser des mots de passe complexes pour différents sites web ou services ; il suffit de mémoriser un seul mot de passe principal. Bien sûr, celui-ci doit être particulièrement robuste, assez facile à mémoriser pour vous et ne doit ni être conservé par écrit ni partagé avec qui que ce soit. (voir la fiche « *Mots de passe* »).

La sécurité de cette base de données peut être encore renforcée en joignant une « clé » (un fichier dont la possession sera exigée, en plus du mot de passe principal, pour accéder aux mots de passe enregistrés).

Téléchargement et installation du logiciel KeePass (Windows)

Comme pour la plupart des autres programmes, vous devez tout d'abord télécharger le logiciel **à partir du site officiel** https://keepass.info/download.html. Choisissez la dernière version disponible, en haut de page.

Une fois le fichier d'installation téléchargé, ouvrez-le pour procéder à l'installation. Une fois celle-ci terminée, vous pouvez créer votre fichier chiffré en cliquant sur le bouton « Créer un nouveau fichier ». Vous aurez alors besoin de choisir un emplacement et de définir un mot de passe principal.

KeePass ne parle-t-il qu'anglais ?

Par défaut le logiciel est en anglais mais vous pouvez télécharger un fichier qui permet le passage en français ici : https://keepass.info/translations.html (de nombreuses autres langues sont également disponibles au même endroit).
Une fois le fichier de langue extrait, placez le dans le répertoire local « C:\Program Files (x86)\KeePass Password Safe 2\Languages » puis ouvrez KeePass > View > Change langage

Téléchargement et installation du logiciel KeePass (Linux ou MacOS)

KeePass peut en principe fonctionner avec ces systèmes. Vous pouvez également recourir à l'une des variantes recensées sur la page officielle (https://keepass.info/download.html), par exemple KeePassXC qui a une interface plus moderne et propose quelques options complémentaires telles que la génération automatique de nouveaux mot de passe (une version Windows est également disponible) : https://keepassxc.org/.

Ajouter des entrées

Une fois que vous avez créé votre fichier chiffré, vous pouvez commencer à ajouter des mots de passe. Pour cela, vous devez cliquer sur l'icône « Ajouter un compte » et saisir les informations requises telles que le site Web, l'identifiant et le mot de passe unique. Une fois ces informations saisies, vous pouvez cliquer sur le bouton « Enregistrer » pour ajouter l'entrée. Si vous souhaitez ajouter des notes supplémentaires à propos de cette entrée, vous pouvez le faire en ajoutant des mots-clés ou des étiquettes. Vous pouvez bien entendu supprimer ou modifier les entrées saisies, par exemple à l'occasion d'une mise à jour régulière du mot de passe demandée par de nombreux services pour des raisons de sécurité.

Sauvegarder le « trousseau de clés »

Tout appareil étant susceptible de connaître une panne, il est vivement recommandé d'effectuer de temps à autre une sauvegarde de votre base de clés : il suffit pour cela d'enregistrer le fichier sous un autre nom et de le conserver en lieu sûr sur un autre appareil. N'oubliez pas de renouveler l'opération après l'ajout de nouveaux mots de passe ou la mise à jour des plus importants !

Cette méthode permet également d'utiliser votre gestionnaire de mots de passe sur différents appareils : par exemple un ordinateur personnel et un smartphone qui reste en votre possession.