Sécuriser ses comptes avec de bons mots de passe

Pourquoi se soucier de son mot de passe

- Si votre compte est piraté, vous n'y avez plus accès, mais quelqu'un d'autre si !

- Certains services contiennent des données plus sensibles que d'autres :
  - messagerie : le plus sensible car c'est depuis sa messagerie que l'on pourra gérer les oublis et changements de mots de passe provenant des autres services
  - banque
  - sites marchands, surtout si les informations de votre carte bancaire sont enregistrées
  - réseaux sociaux,...

Comment pirate-t-on votre mot de passe ?

Rare

Malveillance d'un proche qui connaîtrait vos identifiants
→ *ne pas laisser traîner son mot de passe (parlez-en au prince William lors de son passage dans la Royal Air Force !) ni le communiquer à tout le monde…*

Plus commun

Des personnes (appelons-les "pirates") récupèrent des listes entières d'identifiants, le plus souvent en utilisant une faille de sécurité d'un site ou en les achetant auprès d'autres pirates.

Pour trouver le mot de passe associé au compte, ils utilisent des programmes informatiques qui tentent de le découvrir en utilisant des dictionnaires, des listes de combinaisons courantes et en multipliant les combinaisons possibles, jusqu'à trouver le bon mot de passe.
On parle d'attaques de "**force brute**". Nous y reviendrons plus loin
→ *avoir un mot de passe long et/ou complexe*

De plus en plus commun

Les pirates arrivent à subtiliser des noms d'utilisateur et mots de passe en utilisant des failles de sécurité de sites Internet peu ou mal sécurisés
→ *vérifier régulièrement si des sites sur lesquels vous disposez de comptes se sont fait pirater :*

Un site reconnu et très utile : haveibeenpwned.com
Vous indiquez votre adresse mail et il vous indiquera s'il la retrouve dans sa base de données de comptes piratés depuis 2007. Si c'est le cas, changez rapidement votre mot de passe sur le site en question...

Pourquoi moi ?

- **Les pirates n'ont rien contre vous !** Ils ne vous connaissent pas et vous ne serez pour eux qu'une personne piratée parmi des millions d'autres.

- **Votre mot de passe les intéresse**. Une fois récupéré le mot de passe d'un site ainsi que l'identifiant (souvent votre adresse mail), les pirates utilisent des programmes informatiques qui vont tester cette combinaison "identifiant + mot de passe" sur de très nombreux autres sites. Si vous utilisez le même mot de passe pour plusieurs sites, vous facilitez grandement le travail des pirates !

- **Certaines de vos données sont sensibles** : informations bancaires, numéros de CB, numéro de sécurité sociale, données médicales… Elles peuvent soit être utilisées pour vous dérober de l'argent, soit être revendues sur Internet (de 1$ le mot de passe à quelques dizaines de dollars pour un numéro de CB). Attention lorsqu'un site marchand vous propose d'enregistrer vos coordonnées bancaires pour éviter d'avoir à les ressaisir, le site peut se faire pirater et les données être récupérées.

- **Les données dérobées, même peu sensibles**, sont revendues en masse à des personnes qui les utiliseront pour vous envoyer des mails ciblés pour lesquels vous serez moins vigilants. Ces mails, contenant un lien ou une pièce jointe vérolée, leur permettront alors au cas où vous cliquez dessus d'installer un programme malveillant qui pourra crypter votre ordinateur et vous demander une somme d'argent pour retrouver vos données (on parle de ransomware)

C'est quoi un mauvais mot de passe ?

Pour les inconscients

- Les listes des mots de passe les plus utilisés (dans plusieurs langues) étant disponibles sous forme de fichiers sur Internet, vous devez les éviter (azerty, 123456, password, toto,…), ils sont vraiment trop faciles à trouver !

- Utiliser le même mot de passe pour tous (ou quasiment tous) ses comptes, surtout pour les services les plus sensibles.

Les fausses bonnes idées

- utiliser des informations personnelles en se disant que "personne ne le sait donc personne ne pourra le deviner" (surnom, club de foot préféré, prénom des enfants,…) Pour les logiciels utilisés pour trouver votre mot de passe, les mots n'ont pas de "sens", ce ne sont que des combinaisons de caractères

- mettre un numéro à la fin du mot de passe (département, code postal, année ou date de naissance,...)

- remplacer des lettres par des caractères spéciaux (@ pour la lettre a, 0 pour la lettre o,…)

C’est quoi un bon mot de passe ?

Les programmes utilisés pour "deviner" votre mot de passe nécessitent de tester des millions de combinaisons de lettres, de chiffres et de caractères spéciaux.
Plus les ordinateurs utilisés par les pirates sont nombreux et puissants, plus ils sont capables de tester de combinaisons à la fois et donc de trouver votre mot de passe rapidement. Si votre mot de passe est "toto12", n’importe quel ordinateur utilisant le bon logiciel peut le trouver en moins d’1 seconde.

Pour qu’il soit impossible à trouver (donc que cela prenne trop de temps pour être trouvé), votre mot de passe doit être :

- **soit long** (au minimum 12 caractères) et nécessitant des combinaisons de caractères complexes, illogiques ou logiques.
  → Exemple : ***b78@ui’!HOr-q*** *(caractères rentrés au hasard)*
  → Exemple : ***1tvmQ2tl’A*** *(un tiens vaut mieux que deux tu l’auras) ou* ***ght8CD%E7am*** *(J’ai acheté 8 CD pour 100€ cet après-midi)*

- **soit <u>très</u> long** avec des mots simples. On parle alors de "**phrase de passe**", qui sont plus simples à retenir que des mots de passe complexes et qui sont, par le nombre de caractères utilisés, bien plus difficiles à trouver pour un ordinateur, le plus puissant soit-il.
  → Exemple : *Longtemps je me suis couché de bonne heure.*

L’idéal est donc d’utiliser une phrase de passe… mais **différente pour chaque site** !
Comme vous n’allez pas utiliser toutes les phrases d’ "A la recherche du temps perdu", vous pouvez utiliser la même phrase pour des sites contenant des données peu sensibles et vous fendre d’une phrase de passe particulière pour chaque site sensible !

Une autre solution : **modifier un bout de votre phrase de passe en fonction du service utilisé**
→ Exemple : *Longtemps je me suis couché de bonne heure sur la Camif* (pour votre compte Camif)
Vous faites ensuite de même pour votre compte MAIF, MGEN, Casden, Télérama,...

Pour vous aider

Tester son mot de passe

Une fois que vous avez trouvé votre mot de passe, vous pouvez en tester la solidité sur certains sites.

Attention : même si les sites vous expliquent qu’ils ne retiennent pas votre mot de passe ou qu’ils le cryptent lorsque vous le testez, il vaut mieux tester un mot de passe similaire (même longueur, même composition)

→ **Nothing2hide** (nothing2hide.org/fr/verifier-la-robustesse-de-votre-mot-de-passe)
→ **Kaspersky password checker** (password.kaspersky.com/fr)

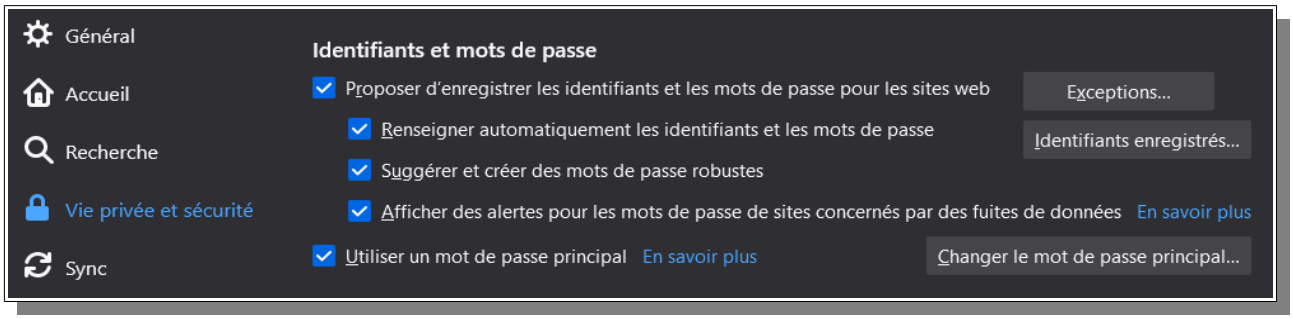
Utiliser un gestionnaire de mot de passe

De plus en plus utilisé, le gestionnaire de mot de passe est un logiciel (sur votre ordinateur), une application (sur votre smartphone) ou une option de navigateur qui enregistrera pour vous de façon cryptée vos identifiants et vos mots de passe.

Une fois déverrouillé, le gestionnaires de mot de passe vous proposera de remplir automatiquement ces informations lorsque vous naviguerez sur les sites dont vous avez un compte.

Pour être déverrouillé, le gestionnaire aura besoin d'un mot de passe qui, vous vous en doutez, devra être très solide !

→ **Firefox** propose un gestionnaire de mot de passe dans ses options :



Ce gestionnaire de mot de passe est associé à une application mobile (**Firefox Lockwise** - mozilla.org/fr/firefox/lockwise) pour votre smartphone.

Pour retrouver vos identifiants et mots de passe sur votre ordinateur personnel, votre smartphone et même sur votre lieu de travail (pensez à la version portable de Firefox sur une clé usb ou dans votre espace personnel), n'hésitez pas à vous créer un compte sur Firefox : cliquer sur Menu puis "Se connecter à Firefox".

→ Un gestionnaire de mot de passe gratuit et opensource, certifié par l'ANSSI : **Keepass** (keepass.info)
→ Un autre gratuit et opensource : **Bitwarden** (bitwarden.com)
→ D'autres solutions propriétaires ayant pignon sur rue : **Lastpass**, **Dashlane**, **Keeper,...**

Utiliser la double authentification (un peu plus complexe à mettre en œuvre)

De très nombreux services proposent d'activer la double authentification, ce qui peut être judicieux pour des services très sensibles (messagerie, site bancaire,…)

Le principe est simple : une fois rentrés votre identifiant et votre mot de passe, vous devez valider une information sur votre smartphone :

- soit en cliquant directement sur celui-ci (ex. les services Google le proposent)
- soit en entrant sur le site une suite de chiffres fournie aléatoirement par votre smartphone grâce à une application dite "OTP"

L'idée c'est que même si on vous dérobe votre mot de passe, il faudra aussi votre smartphone pour accéder au service.