Les mots de passe : « Explications »

Les sites Internet sur lesquels vous avez des comptes stockent vos logins et mots de passe dans leurs bases. A moins de ne pas créer de compte du tout, vous n'avez donc pas d'autre choix que de faire confiance à ces sites pour le stockage et la sécurisation de vos mots de passe.

Vous aurez donc beau mettre en œuvre les meilleures pratiques de sécurité pour le stockage de vos mots de passe, ça n'empêchera pas qu'ils puissent être récupérés par des hackers dans les bases des sites auxquels vous vous connectez ! D'ailleurs il ne serait même pas étonnant du tout qu'au moins un de vos mots de passe ait déjà été volé, sans que vous le sachiez. Jugez par vous-même :

Quelques exemples qui font froid dans le dos

Dans cette note d'octobre 2017 du site de Oath, qui a racheté Yahoo en juin 2013, on apprend que plus d'un milliard de comptes Yahoo ont subi un vol de données en août 2013 !
Dans une note de 2016 d'Uber, on apprend que des données personnelles de plus de 57 millions d'utilisateurs dans le monde ont été dérobées.

Selon le rapport annuel 2018 de Cisco sur la cybersécurité, les téléphones mobiles sont les appareils les plus difficiles à protéger.

Selon cet article de décembre 2017 du site medium :
En parcourant le « dark web » à la recherche de données volées, dévoilées ou perdues, 4iQ (*) a découvert un fichier contenant une base de données de 1,4 milliard d'informations d'authentification en texte clair – la plus grande base de données globale trouvée à ce jour sur le Web « sombre » !

(*) 4iQ est une société spécialisée dans l'investigation et l'alerte sur les problèmes de sécurité
Dans ce rapport de 2015 de Telesign (une entreprise spécialisée dans l'authentification et la notification), concernant une étude sur un échantillon de 2000 consommateurs américains et anglais, on peut lire que :
Au cours de la dernière année, 40% des consommateurs ont subi un incident de sécurité (ont été notifié que leurs informations personnelles avaient été compromises, qu'ils avaient un compte piraté ou qu'ils avaient un mot de passe volé) et 70% ont changé leurs mots de passe en conséquence.

En 2018, vous avez sans doute également entendu parler du scandale Facebook – Cambridge Analytica. Cette société a recueilli des données personnelles de quelques 87 millions d'utilisateurs de Facebook à partir de 2014 !

Tous ces exemples montrent que le vol de données sur Internet est massif. Nous sommes tous tributaires des entreprises auxquelles nous confions nos données et il est illusoire de penser que nous sommes à l'abri…

Un excellent test à faire

Mozilla fournit un service intéressant appelé Firefox Monitor.

Test d'une adresse électronique dans Firefox Monitor

Il vous permet de savoir si des données personnelles vous concernant ont déjà été compromises dans des fuites de données liées à des attaques de cybercriminels. Pour cela, rien de plus simple : allez sur la page de l'outil, saisissez votre adresse email et cliquez sur le bouton Vérifier. La page affichera alors la liste des comptes associés à votre adresse électronique qui ont fait l'objet de fuites de données, ainsi que les types de données compromises.

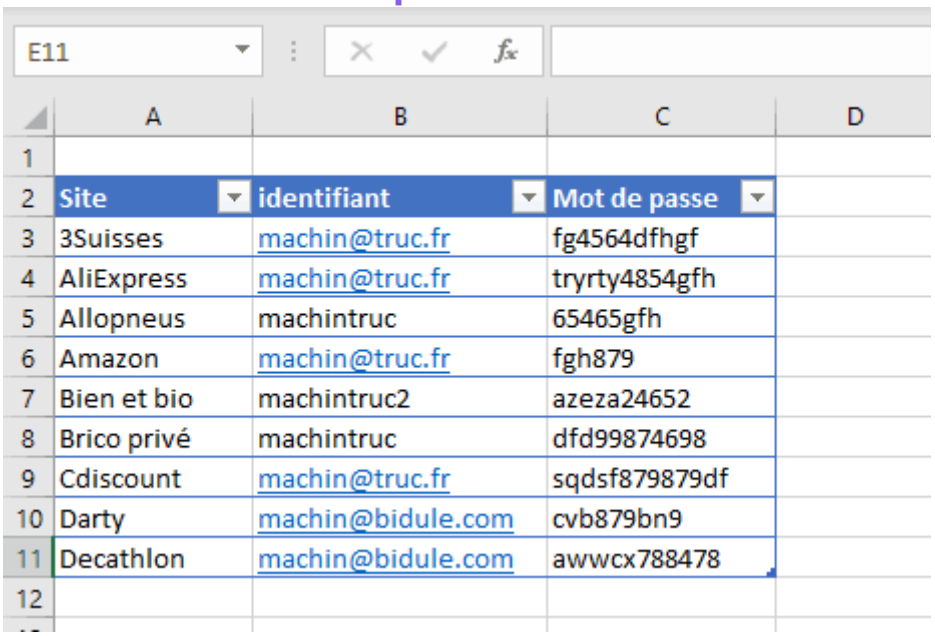
C'est ainsi que j'ai découvert par exemple que des données me concernant ont été compromises dans trois fuites de données. Et surtout que mon mot de passe le plus important a été compromis par une attaque envers Adobe en 2013. Avant d'apprendre cela, j'ai utilisé ce mot de passe pendant trois ans sur plusieurs sites… D'où l'importance de ne pas utiliser le même mot de passe pour plusieurs sites !

Faites le test à votre tour. Mais même si le rapport est vierge, cela ne prouve malheureusement pas que vos données personnelles n'ont jamais été compromises. Mozilla se base sur les données de Have I been Pwned qui recense les attaques connues. Il est cependant probable que beaucoup d'attaques n'aient jamais été révélées.

Les erreurs à éviter concernant votre propre gestion de mots de passe

Ce n'est pas parce que vos données sont à la merci des attaques sur le web qu'il est inutile de gérer correctement vos mots de passe, au contraire. De plus, la sécurité n'est pas le seul élément à considérer. Avant de voir les solutions possibles, voyons les erreurs à éviter.

Stocker ses mots de passe dans un fichier local



	A	B	C	D
1				
2	Site	identifiant	Mot de passe	
3	3Suisses	machin@truc.fr	fg4564dfhgf	
4	AliExpress	machin@truc.fr	tryrty4854gfh	
5	Allopneus	machintruc	65465gfh	
6	Amazon	machin@truc.fr	fgh879	
7	Bien et bio	machintruc2	azeza24652	
8	Brico privé	machintruc	dfd99874698	
9	Cdiscount	machin@truc.fr	sqdsf879879df	
10	Darty	machin@bidule.com	cvb879bn9	
11	Decathlon	machin@bidule.com	awwcx788478	
12				

Gestion des mots de passe dans un fichier Excel

A priori, on pourrait penser que mémoriser ses mots de passe chez soi dans un carnet ou dans un fichier local non synchronisé sur Internet (via OneDrive, Google Drive ou autre) et une solution acceptable. En utilisant un nom de fichier discret et une extension non reconnue par les applications courantes on peut brouiller davantage les pistes en cas d'intrusion d'un hacker sur notre ordi.

L'intention est louable, mais cette solution est très médiocre pour plusieurs raisons :

Une solution peu sûre et pas pratique du tout

Avant toute chose, gardez à l'esprit que vos mots de passe sont aussi stockés sur les serveurs des sites sur lesquels vous avez créé un compte. Ils sont donc en fait **déjà** présents sur Internet. Vouloir à tout prix garder votre fichier en local ne devrait donc pas être votre préoccupation majeure.
Ensuite, si les hackers sont capables de voler des données à des entreprises telles que Facebook, qui dépensent des millions de dollars dans leurs systèmes de sécurité, croyez-vous que votre ordinateur soit à l'abri ? Les logiciels espions déployés sur les ordinateurs individuels sont légion.

Surtout, c'est une solution très peu pratique (et même carrément chiante 😉) à utiliser au quotidien, car :

- Ça vous oblige à maintenir une liste dans laquelle il faut noter le nom du site, l'identifiant et le mot de passe pour chaque site sur lequel vous êtes inscrit(e). Qui n'a jamais oublié de compléter ce fichier après s'être inscrit(e) sur un nouveau site ?

- C'est pénible d'avoir à ouvrir le fichier à chaque fois qu'on va sur un site pour lequel on ne se rappelle pas le mot de passe. Ça incite fortement à utiliser le même mot de passe pour tous les sites, ce qui n'est d'ailleurs pas toujours possible et en plus très mauvais pour la sécurité, comme nous allons le voir plus bas.

- Si vous naviguez sur Internet aussi depuis votre smartphone, comment faire pour accéder à vos mots de passe ? Copier le fichier sur votre smartphone ? Dans ce cas, ça vous fait oblige à mettre à jour deux fichier. En plus, le niveau de sécurité sur un smartphone est bien pire que sur un ordi…

Un moindre mal

Quand j'ai eu un second ordinateur, j'ai été confronté à ce problème de partage et de mise à jour du fichier de mots de passe. Pour le résoudre, j'ai opté pour une feuille OneNote protégée elle-même par un mot de passe assez complexe. Cela me permettait d'y avoir accès sur n'importe quel matériel (y compris mon smartphone), même en dehors de chez moi, car mes blocs-notes OneNote sont stockés sur OneDrive.

Cet article devrait aussi vous intéresser : Bitwarden, un gestionnaire de mots de passe puissant et gratuit

Cette solution est un moindre mal, car elle a l'avantage d'être assez facile à mettre en œuvre, mais elle n'échappe pas aux deux premiers inconvénients listés précédemment. Patience, nous allons bientôt voir d'autres solutions plus puissantes !

Utiliser un même mot de passe pour plusieurs sites

En stockant vos mots de passe dans un fichier, vous aurez inévitablement tendance à utiliser un même mot de passe pour plusieurs sites, par commodité (pour ne pas dire paresse 😉). Si vous poussez le bouchon encore un peu plus loin, vous vous contenterez de mémoriser deux ou trois mots de passe « universels », et hop ! même plus besoin de consulter le fichier ! Hmmm, du coup, il sert à quoi le fichier… ? lol

Rassurez-vous, vous n'êtes pas le ou la seul(e) à faire ça… Dans le rapport de Telesign de 2015, on peut lire ceci :

Les consommateurs ont en moyenne 24 comptes en ligne, mais n'utilisent que 6 mots de passe uniques pour les protéger.

73% des comptes utilisent des mots de passe dupliqués.

Les consommateurs changent rarement leurs mots de passe. Près de la moitié (47%) utilisent un mot de passe qui n'a pas été modifié depuis cinq ans ou plus et 77% ont un mot de passe qui a au moins un an.

En revanche, ce n'est pas parce que la majorité des gens adoptent de mauvaises pratiques qu'il est bon de continuer à faire de même…

Pourquoi est-ce une mauvaise pratique ?

Imaginons que vous ayez un compte Amazon sur lequel vous avez enregistré votre carte bancaire pour ne pas avoir à la ressaisir à chaque fois (exemple purement fortuit 😉). Imaginons aussi que vous utilisiez le même mot de passe avec un autre site marchand moins connu, mais aussi moins sécurisé et donc plus facile à hacker. Si un hacker attaque ce site et récupère les adresses email et les mots de passe des clients, que croyez-vous qu'il va essayer d'en faire ?

Si c'est un « petit hacker », il va essayer de **les utiliser sur le site en question et aussi sur des sites marchands plus connus** style Amazon, Cdiscount, Rue Du Commerce…etc. Si vous avez enregistré une carte de crédit sur ce site, c'est le jackpot !
Si ce sont des gens plus malins, ils vont essayer de **revendre ces informations** à d'autres organisations malveillantes de plus grande envergure. C'est comme que se constituent des fichiers de plus d'un milliard de comptes sur le web underground…
En synthèse, vous l'aurez compris : **utiliser des mots de passe différents pour tous les sites est vivement recommandé**. A minima, si vous utilisez un même mot de passe pour plusieurs sites, faites-le pour des sites sur lesquels vous ne stockez pas d'autres données confidentielles (carte bancaire ou autres…)

Utiliser des mots de passe trop simples

Quitte à être paresseux, autant l'être jusqu'au bout ! Mémoriser des mots de passe complexes, c'est trop difficile, alors hop ! on prend sa date de naissance ou le prénom de sa fille et le tour est joué !

J'avoue, même moi j'ai fait ça pendant longtemps, alors que je travaillais déjà dans l'informatique et que j'étais sensé être un peu plus averti sur les problèmes de sécurité informatique que la ménagère de 50 ans ou le papy qui se met à Internet… 😊

Mais il n'est jamais trop tard pour bien faire. Je dois encore avoir aujourd'hui quelques comptes peu importants avec ce genre de mot de passe, mais cette pratique est quasi révolue pour moi. Et surtout, sans que cela me coûte un effort supplémentaire, grâce au gestionnaire de mots de passe que je vous présenterai dans le prochain article !

Pourquoi faut-il éviter les mots de passe trop simples ?
D'une part, parce qu'**ils peuvent être devinés par des humains**.
D'autre part, parce qu'ils sont **très faciles à cracker par les logiciels des hackers**.

Un autre test bluffant à faire

https://www.security.org/how-secure-is-my-password/

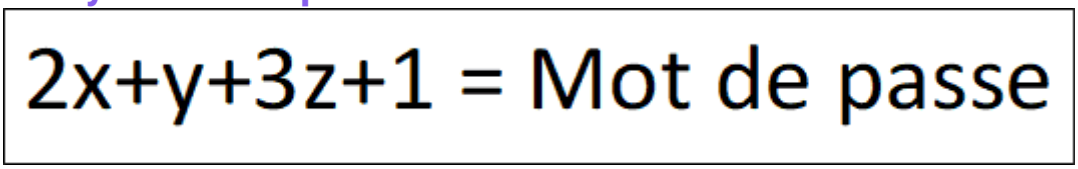
Sur le site https://www.security.org/ , vous pouvez tester le niveau de sécurité de vos mots de passe. Il vous suffit d'en saisir un, et le site affiche le temps qu'il faudrait à un ordinateur pour le trouver.
Voici deux résultats assez éloquents :
Pour trouver le mot de passe 12051988, un ordinateur mettrait seulement 3 millisecondes.
Tandis que pour trouver le mot eBIn5GmLntKm6W, il mettrait 10 millions d'années !
Les valeurs absolues renvoyées par ce site ne reflètent pas vraiment la réalité, car d'une part elles ne tiennent pas compte des temps de latence liés à la connexion Internet. D'autre part, certains sites ont un mécanise de protection qui interdit toute nouvelle tentative de connexion pendant au moins 30 minutes, si les 3 ou 4 dernières tentatives ont échoué. Cependant **c'est la comparaison des temps entre eux qui est vraiment intéressante** (3ms contre 10M d'années selon le mot de passe).
En fait, plus un mot de passe contient de **types de caractères différents** (chiffres, lettres majuscules, lettres minuscules, symboles), plus il est sécurisé.

Les types de caractères comptent plus que leur nombre. Ainsi, le mot « ungrandmotdepasse » qui compte17 caractères est plus facile à trouver que le mot « eBIn5GmLntKm6W » qui en compte 14.

Les solutions concrètes

Après avoir vu les menaces et les erreurs à éviter, nous allons voir maintenant quelles solutions concrètes s'offrent à nous pour gérer nos mots de passe de façon suffisamment robuste.

Un système simple et astucieux



Il vous sera sans doute très difficile de mémoriser vous-même plus de quelques mots de passe, surtout s'ils sont complexes. Cependant, **vous pouvez adopter une logique qui vous permet de retrouver n'importe quel mot de passe pour un site, sans avoir à le mémoriser.**
Par exemple, pour chaque site, vous pourriez utiliser un mot de passe composé de votre année de naissance + les 2 première lettres du nom du site en minuscules + votre jour de naissance + les 2 dernières lettres du nom du site en majuscules + un caractère spécial. Pour le site de Google, ça donnerait quelque chose du genre : 1980go25LE+

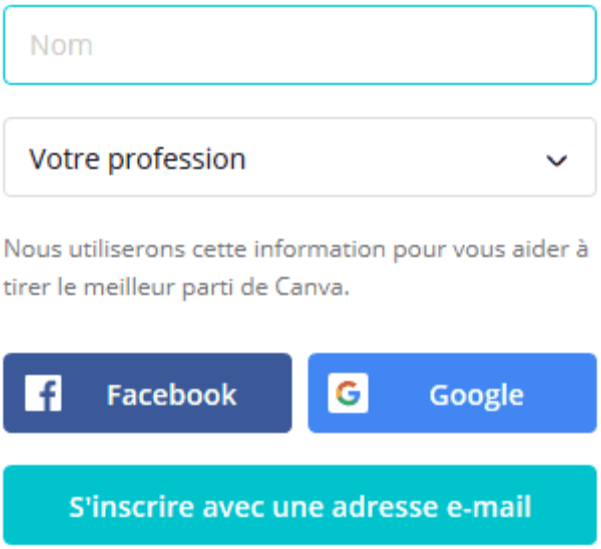
De cette façon, tous vos mots de passe sont relativement différents, complexes et faciles à retenir. Pas besoin de fichier pour les stocker ! Vous avez juste à retenir la convention que vous avez adoptée, une fois pour toutes.
A vous d'inventer votre propre convention. Vous pouvez par exemple utiliser le remplacement de certaines lettres par d'autres caractères (chiffres ou symboles), inclure le nombre de lettres, voyelles ou consonnes du nom du site…etc. Il est important de trouver une logique applicable à tous les cas de figures.

… avec quelques inconvénients mineurs

- Si un site change de nom (exemple : PriceMinister est devenu Rakuten), il faut penser à changer votre mot de passe
- Certains sites imposent des règles sur le nombre et le type de caractères à utiliser dans le mot de passe. Il se pourrait que la convention que vous avez adoptée ne permette pas de les respecter.
- Si votre convention n'est pas assez complexe, vous pourriez être amenés à avoir des mots de passe identiques pour des sites ayant des noms proches.
- Votre mot de passe Google par exemple peut vous servir sur plusieurs sites différents gérés par Google (Gmail, YouTube, Google Analytics…). Il faut dans ce cas se rappeler que c'est bien le mot de passe associé au nom Google qu'il faut utiliser.
- Les mots de passe ainsi définis sont un peu fastidieux à saisir à chaque fois

Mais dans l'ensemble, je trouve que cette solution présente un excellent rapport performance / simplicité.

L'authentification via Facebook, Twitter ou Google



Facebook, Twitter et Google mettent à disposition des autres sites Web des services d'authentification. Ils permettent aux utilisateurs de ces sites de **se connecter sans avoir à créer un nouveau compte**.
Exemple : vous souhaitez laisser un commentaire sur un article d'un blog qui utilise le service d'authentification Facebook Connect. Au lieu de créer un compte sur ce blog, vous pouvez vous connecter avec votre compte Facebook. Votre nom sera alors automatiquement récupéré par le blog depuis Facebook pour s'afficher au-dessus du commentaire. De plus, vous avez la possibilité d'ajouter le commentaire que vous avez écrit sur votre fil d'actualités Facebook.

Ce système présente de réels avantages :

- Il est très pratique pour l'utilisateur : pas besoin de créer un compte supplémentaire pour le site visité. L'authentification sur le site se fait en quelques clics sans rien avoir à taper au clavier.
- De l'information peut être échangée dans les deux sens entre Facebook et l'autre site, ce qui permet à l'utilisateur d'interagir avec ses amis Facebook en dehors de Facebook lui-même.
- Cette technologie est développée par des géants de l'informatique et des nouvelles technologies, qui ont des moyens considérables pour assurer sa fiabilité (ce qui ne veut pas forcément dire qu'ils réussissent…).

Un système qui soulève cependant de grosses questions

Même si Facebook, Twitter et Google ont des moyens considérables pour sécuriser les données, elles sont aussi **les plus attaquées par les cybercriminels** ; et ce ne sont pas toujours elles qui gagnent les batailles… Est-il préférable de confier des données sensibles à une entreprise qui a de gros moyens techniques mais qui est une cible permanente, ou à des entreprises plus petites mais aussi moins sécurisées ?

Cet article devrait aussi vous intéresser : Comment exporter en CSV vos mots de passe Chrome ou Firefox ?

En utilisant les systèmes d'authentification de Facebook, Google et Twitter, **vous leur permettez de savoir à quels sites vous vous connectez et à quelle fréquence**. Est-ce vraiment anodin ? Pouvez-vous faire confiance à l'éthique de ces géantes ? Que sont-elles prêtes à faire de vos données ?

Les récents scandales à répétition dont Facebook a fait l'objet en 2018 (échanges de données, fuites, bugs et failles de sécurité…) incitent vraiment à réfléchir…

En creusant un peu, je suis aussi tombé sur cet article du magazine américain Wired, qui parle de **logiciels capables de récupérer des informations des comptes Facebook** à l'insu des utilisateurs qui utilisent l'authentification Facebook sur d'autres sites …
En ce qui me concerne, j'ai fait le choix de ne pas utiliser cette méthode d'authentification, car elle ne m'inspire pas confiance. En plus, un logiciel de gestion de mots de passe apporte la même facilité d'authentification. J'ai des comptes chez Google, Facebook et Twitter, mais je ne les utilise pas pour me connecter ailleurs. Je préfère cloisonner mes comptes.

La mémorisation des mots de passe par le navigateur

Vous pouvez aussi confer la gestion de vos mots de passe à l'éditeur de votre navigateur (Google pour Chrome, Microsoft pour IE et Edge, Mozilla pour Firefox, Apple pour Safari…)

Si vous créez un compte auprès de l'une de ces firmes, **vous pouvez non seulement laisser votre navigateur mémoriser vos mots de passe, mais en plus ces derniers seront synchronisés sur vos différents appareils**. Cela signifie bien-sûr que vos mots de passe seront stockés quelque part sur les serveurs de la firme en question…
Paramètres pour l'enregistrement des mots de passe dans Chrome et Firefox

Lorsque vous naviguez sur un site sur lequel vous avez un compte, le navigateur est capable de le détecter et de renseigner automatiquement les informations d'authentification à votre place.

J'ai moi-même longtemps utilisé cette solution avec Firefox, mon navigateur préféré. L'avantage est que les mots de passe sont enregistrés sur un compte Mozilla, qui est un fervent défenseur de l'anonymat et du non-flicage sur le web. On ne peut pas en dire de même avec les autres acteurs que je viens de citer…

Les inconvénients de cette solution :

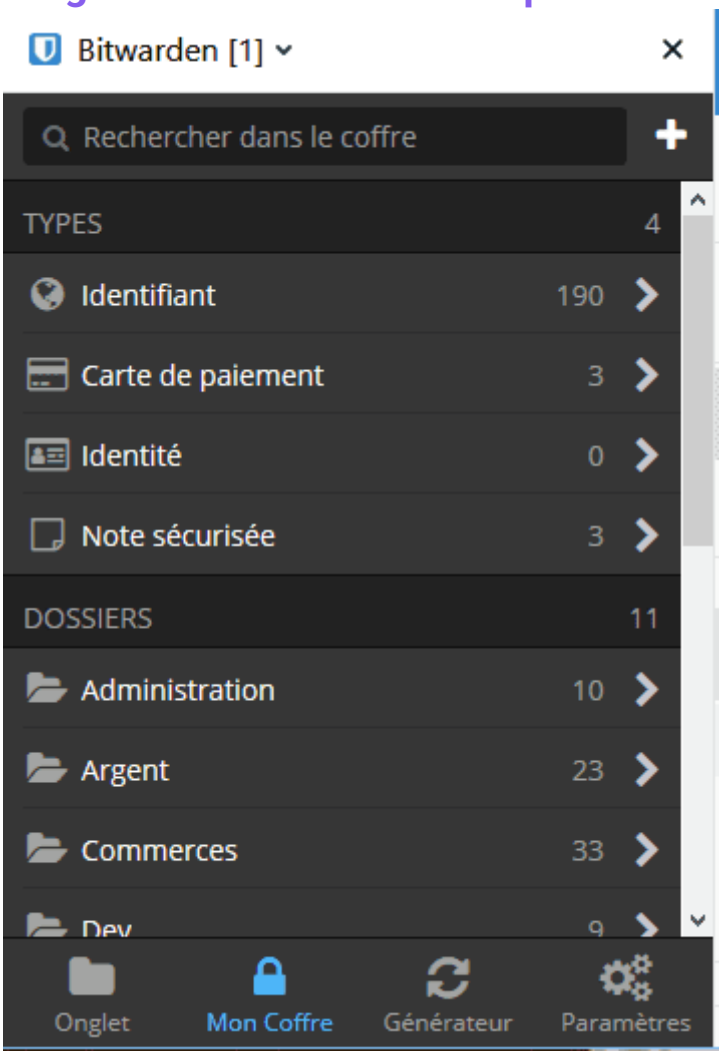
- Vous restez lié(e) à un navigateur unique (celui de la société auprès duquel vous créez votre compte)
- Vous ne pouvez pas enregistrer autre chose que des comptes liés aux sites que vous visitez (exemple : les infos d'une carte bancaire, votre numéro de sécu, un numéro de police d'assurance…)
- Vous ne pouvez pas enregistrer des mots de passe non saisissables au clavier. Typiquement, les banques font saisir des codes sur 4 ou 5 chiffres en cliquant un pavé numérique affiché à l'écran. Ces codes-la ne peuvent pas être mémorisés par votre navigateur
- C'est toujours à vous de trouver des mots de passe suffisamment compliqués et uniques pour chaque site

Les bonnes pratiques

Si vous optez pour cette solution, faites attention aux points suivants :

- Si vous utilisez un ordinateur partagé entre plusieurs utilisateurs (exemple : un ordinateur familial), à moins que vous n'ayez rien à cacher et une confiance aveugle dans tous les utilisateurs :
    - Faites en sorte que chaque utilisateur ait son propre compte sur l'ordinateur ou auprès de l'éditeur du navigateur (Google, Microsoft…). Dans Firefox, vous pouvez protéger vos mots de passe par un mot de passe maître qu'il faut renseigner à chaque fois que vous lancez le navigateur.
    - Déconnectez-vous de votre compte avant de quitter l'ordinateur si vous le laissez allumé
- Mettez à jour régulièrement votre navigateur, car des problèmes de sécurité sont régulièrement découverts et corrigés
- Stockez les autres informations non mémorisables par votre navigateur dans un fichier sécurisé, c'est-à-dire lui-même protégé par mot de passe (Word, Excel et OneNote permettent cela par exemple). Ou bien mémorisez-les si vous êtes vraiment sûr(e) de vous en rappeler (sinon, ça peut être très ennuyeux !)

Un gestionnaire de mots de passe



Panneau du gestionnaire de mots de passe Bitwarden dans un navigateur

Un gestionnaire de mot de passe est un logiciel qui vous aide à mettre en place une gestion très sécurisée des mots de passe, tout en apportant un grand confort d'utilisation.
Voici les caractéristiques et fonctionnalités principales d'un gestionnaire de mots de passe efficace :

- Il permet de **générer automatiquement des mots de passe complexes**, avec le nombre et les types de caractères souhaités.
- Il peut mémoriser vos identifiants et mots de passe pour vos comptes internet **sur tous les types d'appareils (ordinateurs, tablettes, smartphones)**.
- **Il stocke les mots de passe de façon cryptée** sur un serveur web et les protège par un mot de passe maître (le seul que vous ayez vraiment à retenir)
- **Il remplit automatiquement les champs** identifiant et mot de passe dès que vous arrivez sur la page d'authentification d'un site pour lequel vous avez créé et mémorisé un compte.
- **Il s'intègre à votre navigateur** sous forme de module d'extension
- **Il peut mémoriser différents types d'informations confidentielles, pas seulement des comptes de sites Internet** : comptes divers, cartes de paiement, infos administratives…

Finalement, il répond à tous les besoins principaux : sécurisation, centralisation, accès sur plusieurs appareils, confort d'utilisation au quotidien.

Mais attention, le logiciel ne fait pas tout ! Si vous continuez par exemple à utiliser les mêmes mots de passe faibles et pour plusieurs sites, la sécurité restera mauvaise.
Selon une étude réalisée en 2018 par LastPass, un acteur majeur des logiciels de gestion de mots de passe, auprès de 43000 entreprises, le score moyen de sécurité obtenu par les entreprises qui utilisent LastPass est de 52% (ce qui n'est encore pas terrible), mais il était de 23% avant son utilisation.

Mise en place d'un logiciel

La mise en place d'un gestionnaire de mots de passe reste assez simple, car **il est possible d'importer vos mots de passe existants au format csv** pour ne pas avoir à tous les ressaisir. De plus, les navigateurs permettent de générer automatiquement ces fichiers csv.
En revanche, si vous voulez un bon niveau de sécurité, il vous faudra sans doute **modifier la plupart de vos mots de passe pour qu'ils soient plus complexes et uniques**. Pour cela, vous devrez retourner sur chaque site et procéder au changement de mot de passe. Cela peut être long et fastidieux, mais vous n'êtes pas obligé de tout faire d'un coup. Vous pouvez au contraire changer vos mots de passe au fur et à mesure que vous retournez sur vos sites préférez. Vous mettez ainsi progressivement en place une gestion robuste, tout **en bénéficiant dès le départ du confort d'utilisation du gestionnaire** (remplissage automatique, création rapide de nouveaux comptes avec des mots de passe complexes…)
Beaucoup de gestionnaires de mots de passe offrent plusieurs niveaux de prestations : un niveau de base gratuit, et des niveaux avec plus de fonctionnalités mais payants. Vous trouverez sur Internet des comparatifs de ces logiciels, mais trop partiels malheureusement, comme celui-ci ou celui-là.
Dans le prochain article, je vous présenterai de façon détaillée le gestionnaire de mots de passe que j'utilise moi-même depuis l'automne 2018. Il s'agit de Bitwarden, sorti en 2016, très complet et…gratuit !

Bonnes pratiques complémentaires pour la sécurité

En plus d'un système de gestion de mot de passe efficace, voici plusieurs bonnes pratiques que je vous recommande vivement en termes de sécurité :

- Vérifiez que les pages web sur lesquelles vous vous authentifiez sont en https. Celles qui ne le sont pas sont généralement signalées par un cadenas rouge ou autre symbole du même genre
- Mettez régulièrement à jour votre système d'exploitation et vos logiciels, en particulier votre navigateur internet, car de nombreuses failles de sécurité sont régulièrement détectées et corrigées.
- Utilisez un pare-feu et un antivirus pour empêcher les logiciels espions de dérober ou corrompre vos données. Ceux intégrés à Windows 10 sont tout-à-fait suffisants. Pensez à vérifier le résultat de l'analyse automatique qui est lancée de temps en temps.
- Faites de temps en temps le ménage sur votre PC, notamment en vidant le cache de votre navigateur. Pour cela, vous pouvez utiliser un logiciel gratuit tel que Glary Utilities.
- Faites au moins une sauvegarde de vos données les plus sensibles (documents administratifs, de travail…etc.) de temps en temps.

Conclusion

La sécurisation des données et la gestion des mots de passe sont des problématiques sérieuses et complexes à ne pas négliger. Même si vous n'avez jamais eu de problèmes, vous êtes de plus en plus susceptible d'en avoir, car la cybercriminalité ne cesse de s'accroitre. De plus, une gestion de mots de passe pas suffisamment souple peut vous faire perdre beaucoup de temps au quotidien.

Nous avons abordé plusieurs systèmes pour gérer des mots de passe, plus ou moins simples, et présentant chacun des avantages et des inconvénients. Vous l'aurez sans doute deviné, la solution que je préconise est le gestionnaire de mots de passe. Même si sa mise en place nécessite quelques efforts, elle se révèle à l'usage d'une puissance et d'un confort d'utilisation sans pareil.

Dans le prochain article, je vous présenterai de façon détaillée le gestionnaire de mots de passe Bitwarden qui est très complet et gratuit. Même si vous décidez d'utiliser un autre logiciel, vous découvrirez au moins le principe de fonctionnement d'un gestionnaire de mots de passe et ce qu'il peut vous apporter.

En attendant, je serais curieux de savoir comment vous gérez vos mots de passe à l'heure actuelle. Partagez en commentaire, et surtout n'ayez pas honte de ce que vous faites 😉. Moi qui travaille dans l'informatique depuis longtemps, je suis loin d'avoir été exemplaire sur le sujet !