Comptes, identifiants, mots de passe… comment y voir plus clair

Gérer son identité sur internet : comment ça marche, comment s'en servir, comment se protéger, et comment se faciliter la vie

Table of Contents

Les cookies

Les cookies, késako

Dans la vie de tous les jours, il est facile de reconnaître une personne, grâce à son nom, son visage, les lieux dans lesquels on la croise… Mais derrière des écrans, il n'y a rien de tout cela : c'est d'autant plus dur quand c'est une machine qui doit vous reconnaître.

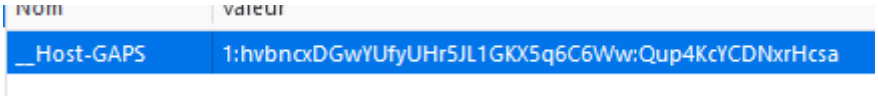
C'est ainsi que dans les années 90 que le « cookie » est inventé. Il se comporte comme un « ticket » ou un bracelet avec un numéro dessus que l'on nous distribue lorsque l'on rentre dans un lieu, et qui permet :

- de prouver que l'on est déjà venu

- de prouver qui l'on est.

Dans les faits, il s'agit d'une suite de charactères aléatoire, qu'un site web fournit lorsque l'on s'y connecte : le navigateur (par exemple Firefox ou Chrome) le stocke alors, et le présente à chaque fois que l'on se connecte au site en question.

En voici un exemple :



Capture d'écran d'un cookie tel qu'affiché dans les « entrailles » du navigateur Firefox.

Il agit donc comme un « mot de passe », plutôt long, et que notre navigateur retient pour nous. Il s'agit juste d'un bout de texte, et non d'un « logiciel » de surveillance, comme beaucoup de gens semblent le penser.

À quoi ça sert

Ce cookie permet donc seulement de nous identifier. Mais dans quel but ?

Imaginons que l'on veuille se connecter avec un identifiant et un mot de passe à un site web protégé . Sans cookie, il y aurait deux manières de faire :

- Retaper le l'identifiant et mot de passe à chaque fois : ce qui est très peu pratique ;

- demander au navigateur de le renvoyer automatiquement à chaque fois que l'on se connecte à une page : ce qui est assez peu sécurisé (imaginez crier votre digicode à chaque fois que vous passez une porte chez vous) ;

Avec un cookie, il suffit de se connecter une seule fois, le site donne alors ce « ticket numéroté » que le navigateur stocke, et il suffit les fois suivantes que ce dernier redonne le cookie : celui-ci peut être configuré pour expirer au bout d'un moment, auquel cas la personne devra se reconnecter.

Le drame

Ces cookies devenant centraux dans l'usage du web, les navigateurs prennent alors l'habitude de stocker à tout va tous les cookies qui leur sont présenter. Certaines personnes et entreprises se rendent alors compte du potentiel de la chose : si l'on donne un cookie au navigateur d'une personne visitant notre site, même si celle-ci ne s'identifie pas, il est alors possible de suivre ses habitudes sur le site : quelles pages elle visite, quels potentiels achats elle souhaite faire,… bref, construire un « profil utilisateur ».

Mieux encore, si le cookie est rattaché à un site « fantôme », et que ce site est caché sur différents sites web, on peut alors surveiller les usages d'une personne à travers le web. Comme si l'on avait un bracelet avec un numéro chaque fois que l'on rentrait dans un centre commercial, et qu'en fonction des magasins que l'on visite, le directeur du centre envoyait des démarcheurs vous interpeller en plein milieu de vos emplettes pour vous proposer *le* produit qu'il vous faut.

Cet abus des « cookies » a mené à trois choses :

- les utilisateurs ont fini par associer « cookies » avec « pistage » ;

- face à ces abus, certains pays ont mis en place des lois obligeant les sites à informer leurs visiteurs qu'ils utilisent des cookies de traçage ;

- des développeurs ont commencé à créer des technologies pour bloquer tout cookie indésirables ;

Un jeu du chat et de la souris, aussi bien technique que légal s'est alors mis en place. Les publicitaires tentèrent de contourner les limitations légales en parlant de « cookies permettant d'améliorer la qualité du site » et techniques en floutant la différence entre un cookie « utile » et un cookie de pistage. En parallèle, les outils de protection de la vie privée pullulèrent.

La réponse : le RGPD

Le dernier chapitre en date dans cette course est l'adoption à l'échelle européenne du « Règlement Général sur la Protection des Données » (ou RGPD), visant entre autres choses à donner la possibilité aux utilisateurs le choix quant aux cookies.

Une notion fondamentale de ce texte est le **consentement libre et éclairé** de l'utilisateur :

- **consentement**, car l'utilisateur a le choix d'accepter les cookies ou non : plus question de simple dire qu'il y a des cookies ;

- **libre**, car il n'est pas possible de forcer l'utilisateur en l'empêchant d'utiliser correctement le site s'il refuse ;

- **éclairé**, car l'utilisateur sait ce qu'il accepte et refuse : plus de définition floue entre les cookies « nécessaires » (pour s'identifier par exemple) et les cookies à but publicitaire.

Dans les faits, entre sa transposition dans les lois de chaque état membre de l'union européenne, les tentatives de contournement et l'inertie du système judiciaire, son respect

reste encore aujourd’hui assez lacunaire. Mais la Commission Nationale de l'Informatique et des Libertés (CNIL) française a déjà depuis infligé des amendes non-négligeables pour non conformité au RGPD à de grandes entreprises comme Google et Facebook.

Aujourd’hui, la plupart des sites affichent désormais un encart lors de la première visite proposant le choix dans les cookies : ces encarts empêchent l’utilisation du site, sont souvent remplis de pièges pour faire accepter les cookies de force, voire demandent carrément un abonnement payant pour refuser les cookies. Aucunes de ces mesures étant en conformité avec le RGPD, menant à une frustration des utilisateurs du web, en attendant que le RGPD soit réellement appliqué.

S’identifier sur internet

Les comptes

Les cookies permettent donc aux sites web de nous reconnaître, aussi bien pour des usages légitimes (comme s’identifier sur un site protégé) ou non (comme le pistage publicitaire). Tout cela se passe dans les entrailles de nos appareils, sans que l’on le sache.

Un de ces usages est donc l’identification : lorsque l’on veut accéder à un site nécessitant de « prouver » qui l’on est pour discuter avec des ami-es, payer des factures, consulter ses papiers administratifs… on utilise donc un « compte », généralement composé d’un *identifiant* et d’un *mot de passe*.

L’identifiant permet de montrer qui l’on est, et le mot de passe de le prouver en fournissant une information que seul nous possédons.

Cet identifiant prend généralement la forme d’une adresse e-mail : et c’est là que les choses se corsent, puisque l’on peut s’identifier sur le site des impôts… avec une adresse SFR, Orange, Gmail, outlook, etc. Cela est d’autant plus confus lorsque l’on utilise l’adresse e-mail donnée par notre Fournisseur d’Accès Internet, qui semble alors être immuable.

Pour clarifier tout cela, il suffit d’imaginer que dans la vraie vie lorsque l’on voudrait s’identifier auprès d’un service comme un hôpital ou un hôtel, nous fournirions notre **adresse de domicile** plutôt que notre nom. Chaque fois que l’on voudrait accéder à un service protégé, on donnerait alors l’adresse de notre maison ainsi que notre mot de passe :

— *Bienvenue à la banque populaire agricole. Que puis-je pour vous ?*

— *Bonjour, j’aimerais consulter mon compte bancaire.*

— *pas de souci, quel est votre adresse ?*

— *43 rue des plantes en pot, 75000 Trifouilli la belle bleue*

— *vous êtes donc Mme Martin : quel est votre code ?*

— *« tropical »*

— *parfait : Il vous reste 1200 euros sur votre compte.*

Cette adresse servant juste à montrer qui l’on est, il est tout à fait possible de l’utiliser comme « identifiant » à plusieurs endroits.

Cette méthode permet, si jamais vous perdez ou oubliez votre mot de passe, de changer son mot de passe en envoyant un mail permettant de le remettre à zéro : tant que vous avez accès à votre boite e-mail, vous pouvez changez le mot de passe même si vous l’avez perdu, et tant que personne d’autre n’y a accès, vos comptes associés à celle-ci

sont sécurisés. Cela se traduirait dans notre exemple précédent par par possibilité de changer son code bancaire en demandant à recevoir un courrier chez nous, que nous pourrions renvoyer avec un nouveau code.

Le problème est en revanche assez évident : si quelqu'un a accès à votre « maison » et donc votre courrier, il peut tout à faire demander de changer tous vos codes. Le code de votre maison (ou sa clef) est donc central dans votre sécurité.

De la même manière, l'adresse e-mail que vous utilisez pour vous connecter sur vos différents sites préférés est donc le cœur de votre identité numérique, et donc de votre sécurité.

Dans les faits, il est tout à fait possible sur internet d'avoir plusieurs adresses e-mails, autre que celle fournie par SFR, Orange, free, ou autre.

Les mots de passe

Un bon mot de passe

Pour protéger tous ces comptes, nous utilisons donc des « mots de passe » : autrement dit une information que nous seuls possédons.

Comme parfois évoqué dans les média, il est important d'utiliser un mot de passe « solide » :

- assez long pour éviter que quelqu'un le devine en essayant des mots de passe au hasard : on parle alors d'attaque par force brute (0000 ? — non. — « 0001 » ? — non plus. Etc)

- peu commun, c'est à dire éviter des mots courants comme 123456789 ou « diamant » ;

- complexes, c'est à dire n'utilisant pas juste des lettres minuscules, mais aussi des chiffres, des majuscules, des caractères « spéciaux » comme « ! », « # », etc.

Le raisonnement derrière cela est simple : un mot de passe de quatre caractères composé uniquement de chiffre n'a que 10 x 10 x 10 x 10 possibilités, soit 10 000 au total. Pour un ordinateur classique capable d'effectuer des millions voire milliards d'opérations par seconde, c'est du gâteau. Si l'y a ne serait-ce un caractère spécial dans le mot de passe, le pirate ne connaissant pas le mot de passe est alors obligé d'essayer plusieurs centaines de possibilités par lettres, soit 255 x 255 x 255… ce qui fait beaucoup plus.

Si vous souhaitez vous faire une idée, vous pouvez essayer différents mots de passe, avec différentes longueurs et caractères, sur le site suivant (ne rentrez pas un de vos vrais mots de passe !) :

https://password.kaspersky.com/fr/

Ces conseils ont été pris au pied de la lettre par la plupart des sites, qui donnent aujourd'hui des consignes toujours plus tordues pour créer un mot de passe, comme un nombre défini de caractères, des minuscules & majuscules, des chiffres, des

hiéroglyphes… etc. Cette méthode s'avère contre productive, car elle engendre de la frustration de la part des utilisateurs, qui utilisent alors le même mot de passe partout, et ont généralement du mal à s'en souvenir.

Une solution partielle à cela est d'utiliser (**quand le site le permet**) des phrases de passe plutôt que des mots de passe, composées de mots aléatoire. Il est beaucoup plus facile de se souvenir que son « mot » de passe facebook est « *uneautruchefaisantduski* », qui est assez imagé, plutôt que « *34gghap$42Ghtes* ».

En plus de cela, on conseille généralement de faire des mots de passe :

- impersonnels, c'est à dire éviter d'utiliser sa date de naissance ou le nom de son animal de compagnie, des informations qui pourraient être trouvées en recherchant assez sur la personne ;

- différents entre chaque site, si l'on se fait avoir sur un site, les pirates n'auront qu'à essayer ce mot de passe sur d'autres sites sinon ;

En plus de cela, certains sites utilisent de plus en plus des méthodes de connexion « sans mot de passe ». Cela passe généralement par un compte unique faisant autorité, comme par exemple en se connectant en utilisant son compte Google ou facebook. Le site demandera alors directement à ces derniers s'il s'agit bien de vous. Cela engendre des risques pour la vie privée, ainsi qu'un compte unique qui s'il est piraté expose tous vos comptes, mais cela évite de devoir retenir trop de mots de passes.

Une autre méthode que l'on trouve plutôt sur les appareils eux-mêmes plus que sur les sites est l'authentification par « biométrie », en utilisant la forme du visage, les empreintes digitales, etc. Le problème de cette dernière méthode est que si votre identité biométrique est volée par quelqu'un, il n'y a aucun moyen d'en changer.

Se simplifier la vie : les gestionnaires de mots de passe

Pourquoi utiliser un gestionnaire de mots de passe

Il existe en vérité une autre méthode pour se simplifier la vie tout en gardant le contrôle sur sa vie numérique : les « gestionnaires de mots de passe ».

Il s'agit dispositif permettant de stocker ses informations de connexion (identifiants et mots de passe) et donc de maintenir des mots de passe solides tout en ayant pas à s'en à s'en souvenir.

À noter qu'on ne parle pas ici nécessairement d'un logiciel : il est tout à fait possible d'utiliser un simple carnet en papier.

L'important est de considérer deux choses : les hasards de la vie, et son « modèle de menace ».

Concernant les premiers, il s'agit de s'assurer qu'aucun accident ne puisse détruire votre gestionnaire : dans le cas d'un carnet en papier, un incendie domestique, dans le cas d'un logiciel, une panne de l'ordinateur. Le meilleur moyen est donc de maintenir une copie des mots de passe, soit en ayant un deuxième carnet sur lequel on copie le premier de temps en temps, soit dans le cas d'un logiciel d'assurer que celui-ci crée une sauvegarde. Mieux encore, il est tout à fait possible d'utiliser les deux en parallèle, c'est à dire garder une copie de votre logiciel sur papier.

Pour ce qui est du « modèle de menace », il s'agit simplement de se poser la question de pourquoi et comment des pirates pourraient accéder à vos mots de passe. Si vous n'êtes pas une cible privilégiée (journaliste d'investigation, avocat, etc), il y a peu de chance que quelqu'un vous cambriole juste pour voler vos mots de passe. Votre carnet en papier est donc en sécurité chez vous.

Le plus simple à l'air du numérique reste néanmoins le gestionnaire numérique : un logiciel qui vous permet non seulement de stocker vos mots de passe, mais aussi de les rentrer automatiquement et d'en garder une copie accessible depuis n'importe quel appareil (PC, tablette, smartphone). Cela créer moins de friction à l'utilisation des mots de passe, et permet donc de plus facilement employer des mots de passe solides.

S'il existe des logiciels spécialisés (par exemple bitwarden), les navigateurs web intègrent généralement déjà cette fonction.

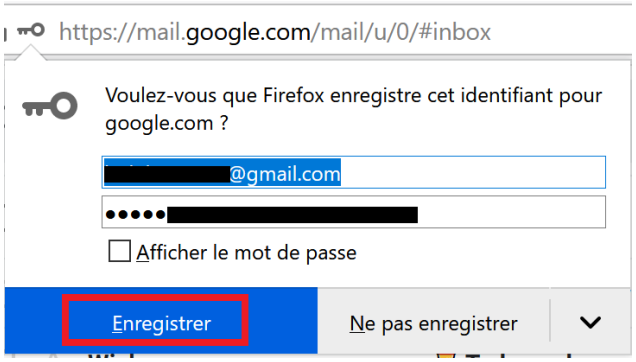
Se pose alors la question de la confiance : peut-on faire confiance à l'éditeur du navigateur en question ? Par exemple, le navigateur Chrome, très répandu, est produit par Google. Google a peu de raisons de voler votre mot de passe, et est très bien sécurisé, mais a la fâcheuse tendance à synchroniser vos données (incluant vos mots de passe) sans vous demander. Cela reste néanmoins un choix raisonnable si vous utilisez ce navigateur au quotidien.

Par souci de vie privée, le navigateur Firefox est plus adapté, car produit par une organisation à but non lucratif. La question de la confiance reste en jeu, et cela vous revient. Mais le tutoriel qui suit s'applique donc pour cette raison à Firefox, et non à d'autres navigateurs.

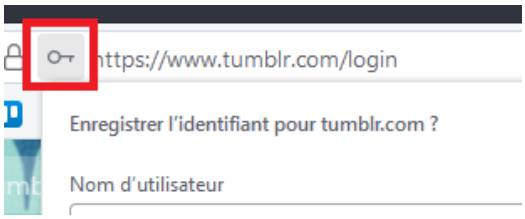
Comment faire : l'exemple de Firefox

Stocker ses mots de passe

Même si ce n'est que la première étape, stocker ses mots de passe dans Firefox est extrêmement simple: il suffit de cliquer sur « Enregistrer » dans la fameuse fenêtre que vous voyez s'afficher après avoir rentré un mot de passe :

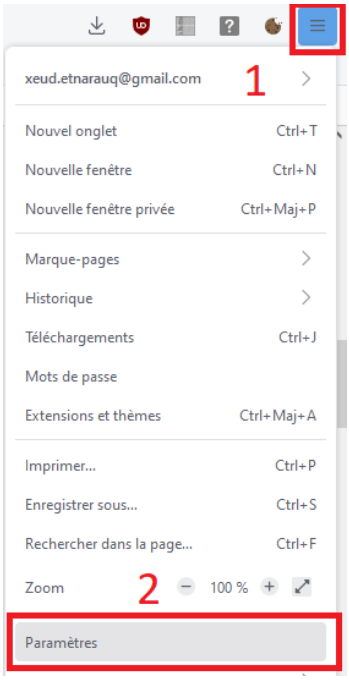


Ou si celle-ci ne s'est pas directement affichée (ou qu'elle s'est masquée après que vous ayez cliqué ailleurs), cliquer sur le symbole en forme de clef juste après votre enregistrement/connexion pour ouvrir celle-ci :

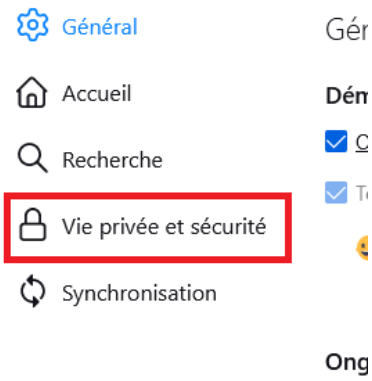


Il est possible que Firefox ne propose pas systématiquement d'enregistrer le mot de passe : certains sites comme les banques ou les sites administratifs ne fonctionnent pas, soit à cause d'un formulaire d'identification non standard empêchant Firefox de détecter la saisie d'un mot de passe, soit à cause d'une politique de sécurité du site (c'est notamment le cas des banques), préférant empêcher tout enregistrement pour diverses raisons (certaines légitimes et d'autres non).

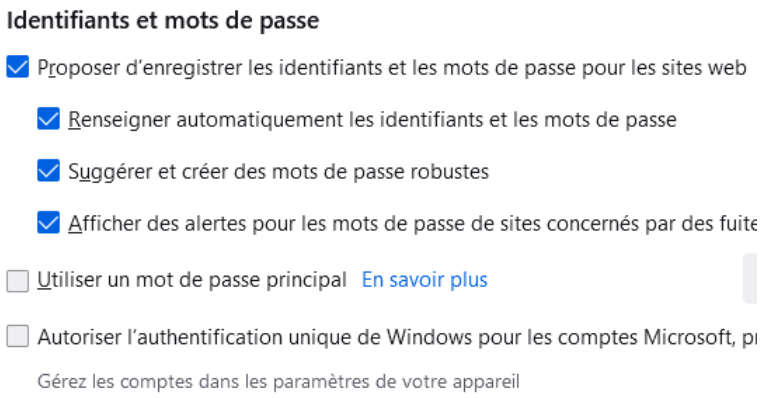
En revanche, si Firefox ne propose pas du tout l'enregistrement (notamment sur les sites connus comme Facebook, Twitter, Gmail, etc), vérifiez que le paramètre est activé en cliquant sur le "menu hamburger" [1] (c'est son nom en graphisme !) en haut à droite, puis sur "Paramètres" [2] :



Se rendre ensuite dans « Vie privée et sécurité » dans le panneau de gauche :

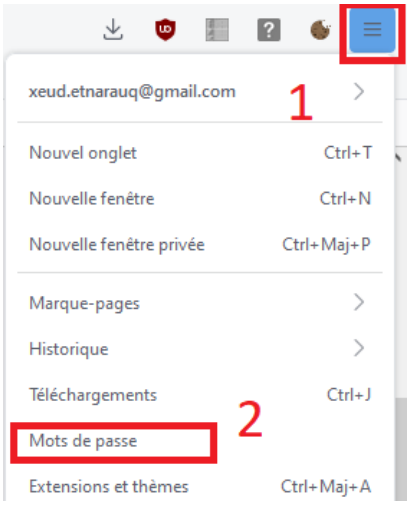


Descendez jusqu'à "Identifiants et mots de passe" et enfin vérifiez que ces cases soient cochées comme indiqué ci-dessous :



Inversement, cela vous permet de désactiver cette fonctionnalité si vous ne l'utilisez jamais.

Mais où vont donc ses mots de passe ? Rien de plus simple à démystifier. Cliquez à nouveau sur le "menu hamburger", plus cliquez sur "Mots de passe" :

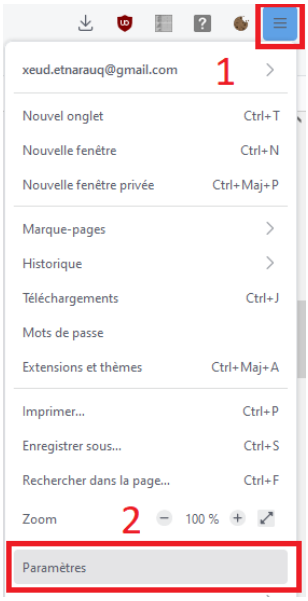


Un onglet s'ouvre alors, listant tous les identifiants, mots de passe, et le site associé. Cela peut également permettre de stocker manuellement d'autres informations comme un numéro de compte.

Protéger ses mots de passe

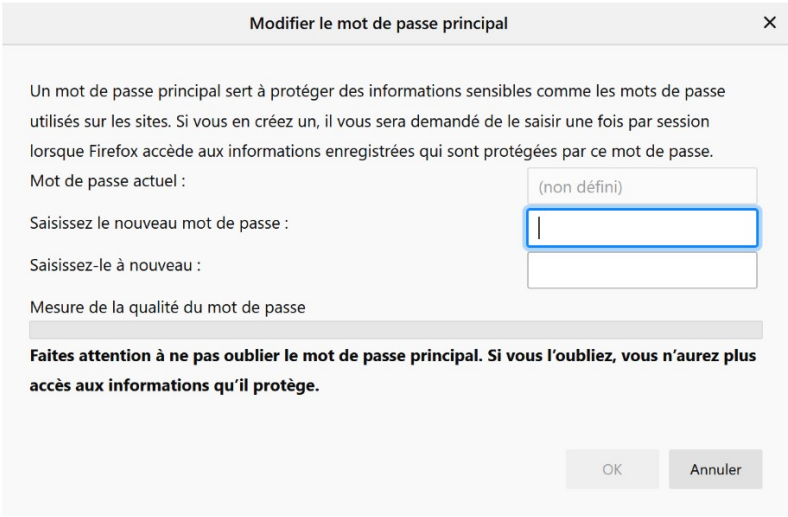
Mais s'il est si facile d'afficher ses mots de passe, n'importe qui ayant un accès physique à mon ordinateur peut le faire ? C'est là qu'entre en jeu le mot de passe principal, qui joue le rôle de code de coffre fort.

Le mot de passe principal permet de protéger tout ces autres mots de passe par un code général qui empêche tout accès indésirable, comme un code de coffre fort. Pour l'activer, rendez-vous à nouveau dans les options en cliquant sur le menu :

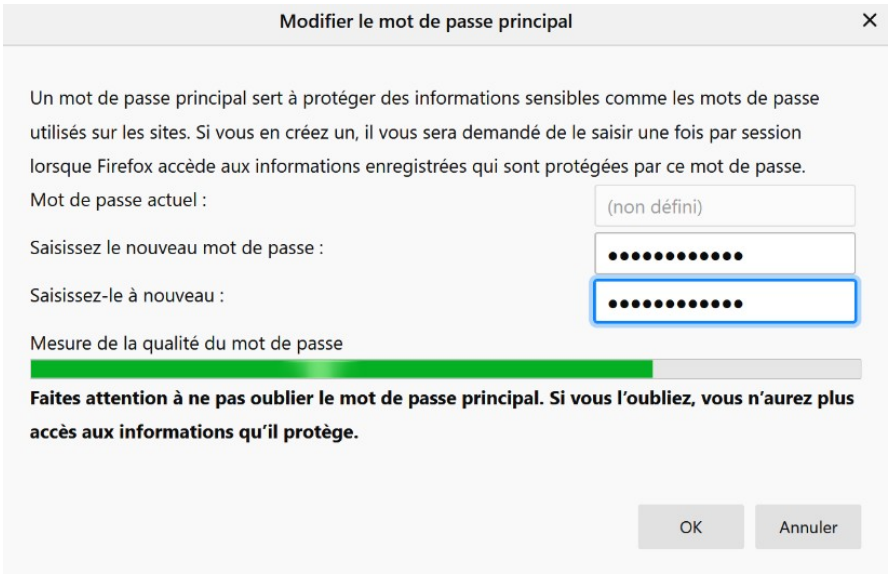


Cliquez sur "Vie privée et sécurité" et descendez jusqu'à "identifiants et mots de passe", et cochez "Utiliser un mot de passe principal" :

Cela aura pour effet d'afficher cette fenêtre :



Le "mot de passe actuel" n'a pas à être rentré, compte tenu qu'il n'existe pas encore. Rentrez un mot de passe identique dans les deux zones suivantes :



Cela permet d'éviter que vous rentriez un mot de passe contenant une faute de frappe. Compte tenu qu'il s'agit du seul et unique mot de passe qui sécurise tous vos comptes (mais également le seul que vous ayez à retenir), choisissez un mot de passe très solide en rentrant par exemple une phrase (on parle alors de **phrase de passe**) plutôt qu'un simple mot. Enfin, **cliquez sur « Ok ».**

Attention : ce mot de passe **ne peut pas être récupéré** en cas de perte (en tout cas pas sans bidouiller et perdre ses mots de passe stocker) et il est donc important de bien le

retenir. Au besoin, **notez le sur un papier gardé en lieu sûr**. Cela est généralement déconseillé, mais votre "modèle de menace" n'inclut sans doute pas que des personnes mal intentionnées viennent spécifiquement rentrer par effraction dans votre maison juste pour voler vos mot de passe, cette technique est donc légitime, pour peu que le **principe de précaution** soit appliqué (éviter de le laisser à la vue de tout le monde, potentiellement le stocker dans un coffre prévu à cette effet, etc).

Ce mot de passe vous sera **demandé une seule fois** à chaque ouverture de Firefox (plus spécifiquement, à la première ouverture d'un site demandant un mot de passe lors de l'utilisation en cours), ou quand vous voudrez consultez vos mots de passe directement via les paramètres.

Désormais, chaque fois que vous **validerez la sauvegarde d'un mot de passe** (ou dans le cas d'un mot de passe déjà existant, **mais que vous désirez modifier**), Firefox **l'enregistrera dans le coffre fort sécurisé** : vous pouvez donc le remplir au fil de l'eau.

Maintenant que vous n'avez plus que le mot de passe principal à retenir, vous pouvez mettre des mots de passe aussi **complexes** que le permettent les sites, et mettre des **mots de passe différents** à chaque compte. Pour les comptes les plus importants (comme les comptes administratifs ou encore votre adresse e-mail, centre de votre vie numérique puisque liée à la plupart de vos comptes), vous pouvez **éventuellement annoter leur identifiant et mot de passe sur le document papier** sur lequel est noté votre mot de passe principal, par principe de précaution. Encore une fois, **les conseils à ce sujet varient beaucoup** dans le monde de la sécurité informatique, mais si vous prenez les **dispositions de sécurité** évoquées plus haut cela ne devrait pas impacter votre sécurité.