

Sécurisez vos mots de passe avec Lastpass

Par Mathieu Nebra (Mateo21)



www.openclassrooms.com

*Licence Creative Commons 6 2.0
Dernière mise à jour le 22/07/2013*

Sommaire

Sommaire	2
Sécurisez vos mots de passe avec Lastpass	3
Pourquoi il ne faut pas utiliser le même mot de passe partout	3
Installer Lastpass	5
Lastpass et ses concurrents	5
Installer Lastpass	6
Utiliser Lastpass pour gérer ses mots de passe	12
Connexion à Lastpass	13
Découvrir Lastpass	14
Enregistrer un nouveau mot de passe sur Lastpass	15
Quand la magie opère : Lastpass remplit les champs de connexion pour vous !	17
Améliorer la sécurité avec la double authentification	19
La Yubikey	19
Google Authenticator	21
Partager	22



Sécurisez vos mots de passe avec Lastpass

Par



Mathieu Nebra (Mateo21)

Mise à jour : 22/07/2013

Difficulté : Facile



1 visites depuis 7 jours, classé 33/807

A chaque fois c'est pareil : vous arrivez sur un site web, vous voulez créer un compte et on vous demande de choisir un mot de passe. Et là vous vous dites : "*La barbe, encore un mot de passe à retenir !*". Vous n'avez pas que ça à faire, déjà qu'il faut retenir le code secret de votre carte bleue et les 150 choses que vous devez faire dans la journée...

Pressé de passer à autre chose, vous utilisez votre mot de passe favori. Vous tapez : "C-H-U-C-K-Y" (oui c'est le nom de votre chien, en tout cas j'espère que ce n'est pas celui de l'un de vos enfants ! 🐶).

Et là, voilà que le site vous fait un affront supplémentaire : "*Veillez rentrer entre 8 et 20 caractères, comprenant au moins une lettre majuscule, une lettre minuscule, un chiffre, un caractère spécial et un symbole mésopotamien*". C'est en général à ce moment précis que vous rêvez de mettre la main sur l'ingénieur geek qui a eu cette idée géniale :



« Mais mais... c'était pour que ton mot de passe soit plus sécurisé ! »

Le problème est pourtant entier : notre ami ingénieur geek a raison de vous demander un mot de passe compliqué. Il a même raison de dire que *vous devriez utiliser un mot de passe complètement différent sur chaque site*.

Mais vous, de votre côté, vous avez aussi raison : vous n'avez pas que ça à faire de retenir 150 mots de passe. Votre mémoire est limitée.

Heureusement, il existe des solutions ! J'en utilise moi-même une qui s'appelle [Lastpass](#), qui m'évite d'avoir à retenir des tonnes de mot de passe. Parce que n'allez pas croire, mais j'étais comme vous avant, j'avais le même mot de passe super simple sur tous les sites que je fréquentais. 🤖

Sommaire du tutoriel :



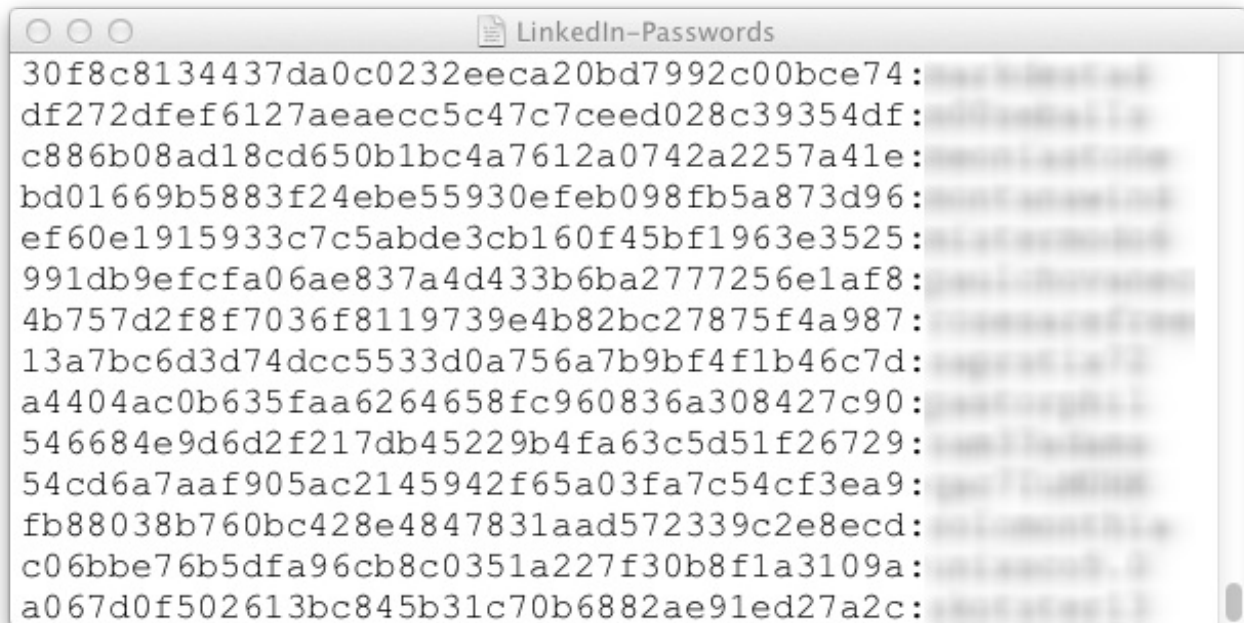
- Pourquoi il ne faut pas utiliser le même mot de passe partout
- Installer Lastpass
- Utiliser Lastpass pour gérer ses mots de passe
- Améliorer la sécurité avec la double authentification

Pourquoi il ne faut pas utiliser le même mot de passe partout

Rassurez-vous, je ne veux pas jouer les moralisateurs. Je comprends tout à fait que ce soit compliqué de retenir plusieurs mots de passe et que vous n'ayez pas envie de le faire. Je vais vous expliquer juste après comment je fais pour gérer mes mots de passe sans me prendre la tête... mais avant ça, j'aimerais juste vous expliquer pourquoi il ne faut pas utiliser le même mot de passe sur plusieurs sites.

On ne le dira jamais assez : **utiliser le même mot de passe partout, c'est mal**. Oui, mais pourquoi ?

Ubisoft, LinkedIn, Last.fm, OVH, Ubuntu, Apple... on ne compte plus les annonces de sites qui ont été piratés. Bien souvent, les pirates cherchent à récupérer les mots de passe, et ils arrivent à extraire des listes géantes comme celle-ci (qui vient de LinkedIn) :



Les

mots de passe volés du site LinkedIn

Rien que sur LinkedIn, ce sont entre 6 et 8 millions de mots de passe qui ont été volés comme ça !

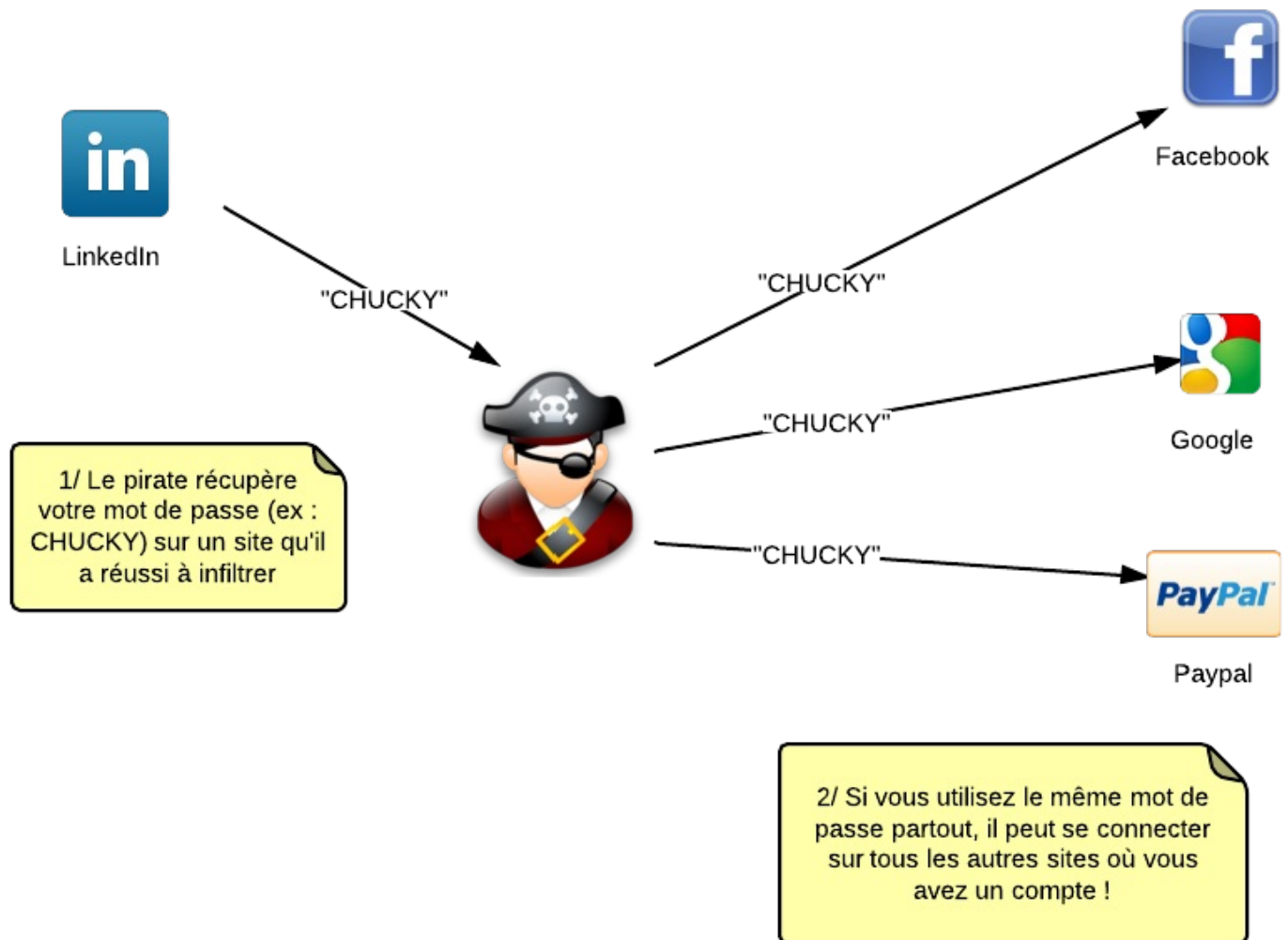


Mmmh... ce sont des mots de passe ça ? On dirait qu'ils sont cryptés...

En effet, fort heureusement la plupart des sites web cryptent les mots de passe... Mais pour les plus simples d'entre eux, il existe des techniques qui permettent de les décrypter. En fait, avec un ordinateur assez puissant, on peut aujourd'hui décrypter un grand nombre de mots de passe simples...

Le plus gros problème ici vient du fait que **beaucoup de gens utilisent le même mot de passe sur plusieurs sites** (oui, je suis sûr que vous y compris 😊). Ou peut-être que vous utilisez un même mot de passe avec de légères variations à chaque fois, mais malheureusement les pirates disposent aussi d'outils pour tester des variations de mots de passe, ce qui ne vous met pas beaucoup plus à l'abri...

Du coup, si vous êtes sur un site comme LinkedIn qui se fait pirater, vous allez devoir changer votre mot de passe sur LinkedIn mais aussi sur tous les autres sites où vous avez mis le même mot de passe : Paypal, Facebook, Google... Sinon, n'importe qui pourra accéder à votre compte sur ces autres sites !



Si vous utilisez le même mot de passe sur plusieurs sites, un pirate pourrait en tirer profit !

Inquiétant ? En fait, il n'y a qu'une seule vraie solution : utiliser des mots de passe longs, très compliqués et surtout **complètement différents** sur chacun des sites que vous visitez. Ca a l'air impossible et pourtant je le fais, laissez-moi vous expliquer comment. 😊

Installer Lastpass

Lastpass et ses concurrents

Avant qu'on ne m'accuse de faire de la publicité exclusive pour Lastpass, je tiens à signaler qu'il existe plusieurs services de gestion des mots de passe :

- [1password](#)
- [KeePass](#)
- [RoboForm](#)
- [StickyPassword](#)
- ... et bien sûr, [Lastpass](#)

Vous pouvez essayer tous les services de cette liste. Si je vous présente Lastpass, c'est tout simplement parce que c'est celui que j'utilise et donc que je connais le mieux. C'est aussi l'un des plus populaires. 😊

Voici ce qu'il faut savoir en quelques lignes sur Lastpass :

- C'est un outil qui sert à gérer tous vos mots de passe en les cryptant de façon avancée pour plus de sécurité

- Vos mots de passe peuvent être synchronisés entre votre ordinateur, votre tablette, votre smartphone...
- Lastpass est gratuit, avec une version payante à 1\$ par mois si vous voulez l'utiliser aussi sur smartphone (ce n'est pas vraiment obligatoire)
- Lastpass peut générer des mots de passe compliqués pour vous, c'est lui qui les retiendra ensuite

Pour résumer Lastpass en une phrase : il vous suffit de **ne retenir qu'un mot de passe pour débloquer tous vos autres mots de passe**. D'où le nom, Lastpass (c'est le "dernier mot de passe" que vous aurez besoin de retenir).



Mais... c'est nul non ? Si tous mes mots de passe peuvent être débloqués grâce à un mot de passe principal, alors un pirate qui connaît mon mot de passe principal a accès à tous mes mots de passe !

Oui.

Mais on peut aller plus loin et augmenter la sécurité : c'est pour cela qu'il est fortement recommandé d'utiliser en plus un générateur de codes secrets que vous portez sur vous. En gros, pour avoir accès à mes mots de passe, il vous faudra utiliser votre mot de passe principal *et* quelque chose que vous possédez (une clé spéciale ou votre smartphone). Si vous n'avez pas les deux, vous ne pourrez rien faire !

(cela veut donc dire que pour me pirater mes comptes il faut deviner mon mot de passe et m'agresser dans la rue pour récupérer ma clé spéciale ! 🤪)

Bref, en faisant les choses correctement comme je vais vous le montrer, vous ne serez pas moins sécurisés, vous serez *beaucoup* plus sécurisés !

Installer Lastpass

Commencez par vous rendre sur <https://lastpass.com> :

The screenshot shows the LastPass website homepage. At the top, there's a red header with the LastPass logo and a language selector set to 'Français'. Below the header, there are navigation links: TÉLÉCHARGER, FONCTIONNALITÉS, RÉPUTATION, SOUTIEN, À PROPOS DE NOUS, and ENTREPRISE. The main banner features the text 'The Last Password You'll Have to Remember!' and a prominent 'Download LastPass' button with a 'FREE' tag. Below the banner, there are logos for various operating systems and a section titled 'c'est PLUS FACILE', 'c'est PLUS SÛR', and 'c'est GRATUIT'.

Le site lastpass.com

Lastpass prend la forme d'une extension pour votre navigateur web (il y en a pour Internet Explorer, Safari, Firefox, Google Chrome, Opera...). Si vous hésitez, le mieux est d'installer la version recommandée : l'installateur universel. Ce programme installera

automatiquement les extensions pour tous vos navigateurs.

LASTPASS POUR WINDOWS (2000/XP/Vista/7/8)



Installeur Universel LastPass pour Windows

Le programme d'installation universel Windows installe les extensions du navigateur pour Internet Explorer, Firefox, Chrome, Safari, et Opera. Il vous permet également de créer facilement un compte LastPass et d'importer vos mots de passe existants. C'est la meilleure façon d'installer LastPass sur Windows. Le programme d'installation 64 bits inclut celui d'IE 32 bits.

Prend en charge Internet Explorer 6+, Firefox 2.0+, Chrome 18+, Safari 5+, Opera 11+.



[TÉLÉCHARGER >](#)

VERSION 2.0.20

L'installeur universel de Lastpass

Premières étapes de l'installation

Lancez ensuite le programme d'installation :



Accueil de l'installation

Vous devez commencer par choisir sur quel navigateur vous voulez installer Lastpass.

Cochez donc les navigateurs que vous utilisez au quotidien. Dans le doute, vous pouvez l'installer sur tous les navigateurs, ça ne pose pas de souci.



Sélectionnez les navigateurs sur lesquels vous voulez installer Lastpass

Lastpass s'installe ensuite (ça ne prend pas très longtemps) :



Lastpass s'installe !

Création du compte

On va vous demander si vous avez déjà un compte ou si vous souhaitez en créer un.

Comme c'est la première fois que vous découvrez Lastpass, il vous faut créer un compte. 😊

LastPass ****

CREER VOTRE COMPTE

Adresse mail

Mot de Passe LastPass
Très bien ! Votre mot de passe est très résistant !

Rappel de Mot de Passe

☒ Je comprends que mes données cryptées seront envoyées à LastPass
Personne à LastPass ne peut lire vos informations confidentielles car elles sont encryptées

☒ J'ai lu et accepté les termes de licence suivants :
[Termes de la licence d'utilisation de LastPass](#)
[Les termes de confidentialité de LastPass](#)

☒ Garder un historique de mes connexions et remplissage de formulaire

Créez votre compte... et choisissez bien votre mot de passe principal !

Votre compte est constitué :

- De votre adresse e-mail
- De votre mot de passe principal (**très important**)

Choisissez soigneusement votre mot de passe principal, c'est lui qui débloquera tous vos mots de passe ensuite. Il faut donc choisir un mot de passe assez long (au moins 10-12 caractères), avec des lettres, des chiffres et des symboles spéciaux (des "+", des "?" ou des accents "â", "è" ...). Voici quelques exemples de mots de passe que je considère comme "corrects" :

- jEf7n!Uv23M
- e4c8hàp22qq
- V?àçg6cDDzxP

- ... (ne prenez aucun de ceux-là, inventez le vôtre !)



Hum... J'en ai marre encore un mot de passe à retenir ! C'est trop long, trop compliqué, je ne le retiendrai jamais ! 😞

Allons, un petit effort. C'est le *seul* mot de passe que vous aurez besoin de retenir !

Au pire, notez-le sur un bout de papier pour quelques jours si vous avez peur de l'oublier, mais ensuite, brûlez ce bout de papier (ou mangez-le ! 😋).

On vous demandera aussi de saisir une phrase qui vous aide à vous rappeler de votre mot de passe. Personnellement, ce type de champ ne me plaît pas et je préfère ne pas le remplir pour éviter qu'une autre personne puisse deviner le mot de passe. Ici, comme le champ est obligatoire, je mets n'importe quoi dedans. 😊

Enfin, Lastpass vous propose gentiment de partir à la recherche de mots de passe non sécurisés sur votre ordinateur :



Lastpass peut récupérer vos mots de passe pour les sécuriser

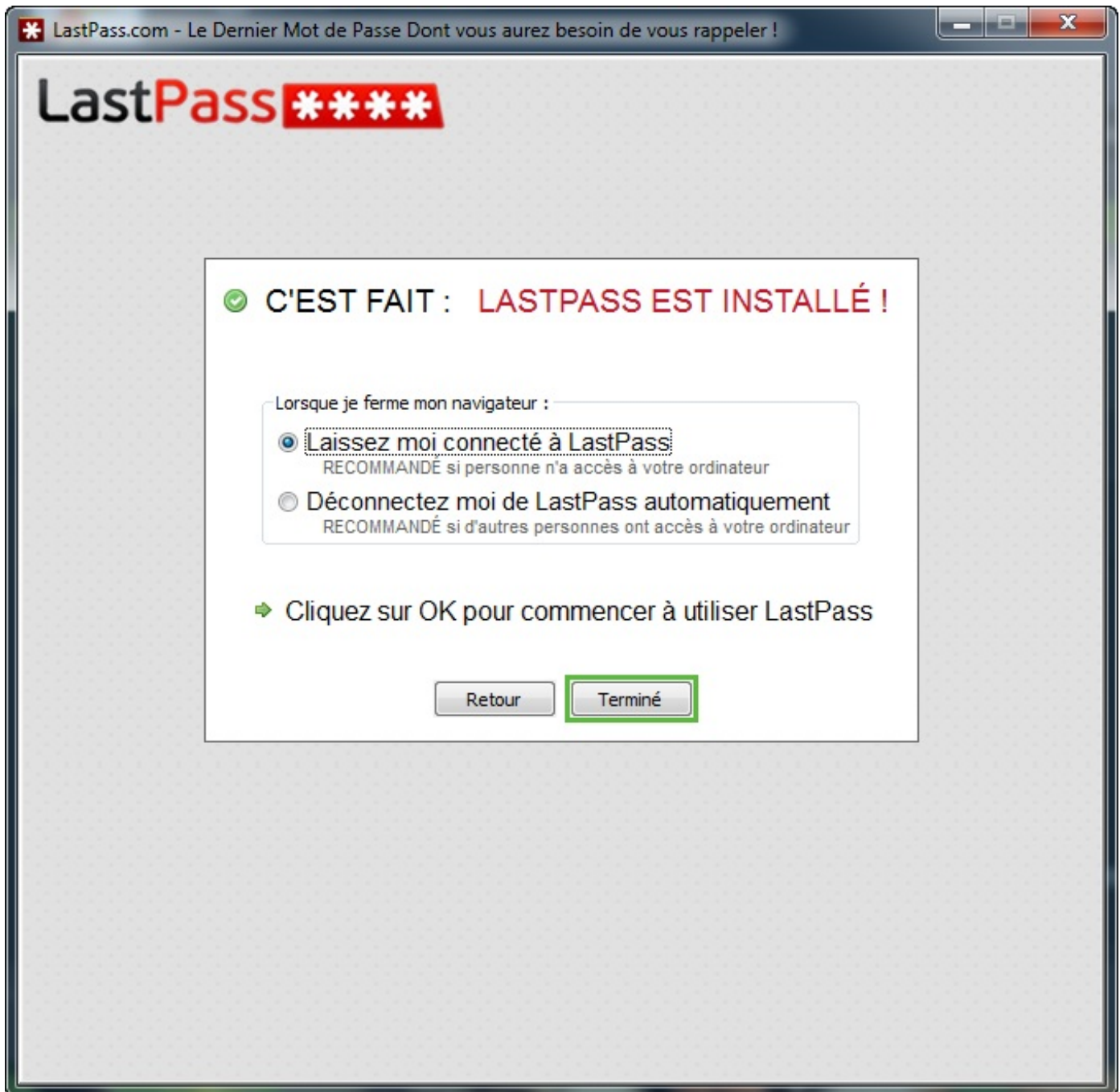
Je vous conseille de laisser Lastpass rechercher des mots de passe non sécurisés. Vous pouvez être surpris du nombre de mots de passe qu'il peut parfois trouver !



Les mots de passe non sécurisés sont généralement enregistrés par les navigateurs web eux-mêmes. Internet Explorer, Chrome, Firefox... Ils ont tous des services qui vous permettent d'enregistrer vos mots de passe, mais ils sont loin d'être aussi sécurisés que Lastpass !

Autre gros avantage de Lastpass : vous pouvez aussi accéder à vos mots de passe depuis n'importe quel navigateur !

Une fois que c'est fait, ouf, vous avez terminé !



Bravo, c'est installé ! :o)

A vous de décider si vous voulez que Lastpass se déconnecte à chaque fois que vous fermez votre navigateur. Je vous recommande la déconnexion automatique surtout si vous êtes sur un ordinateur utilisé par plusieurs personnes à la fois.

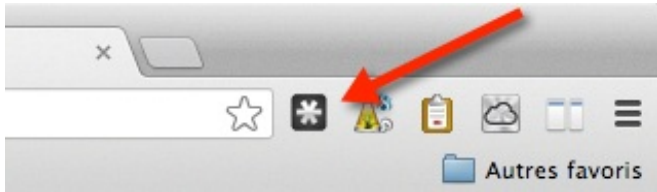
Utiliser Lastpass pour gérer ses mots de passe

Connexion à Lastpass

Maintenant que vous avez installé Lastpass, vous devriez voir une icône s'afficher dans votre navigateur web.



Tous les exemples qui suivent montreront l'extension Lastpass pour Google Chrome. Si vous avez un autre navigateur, il peut y avoir quelques légères différences, mais le principe reste le même.



Cliquez sur l'icône grisée de Lastpass pour vous connecter

L'icône de Lastpass est grisée quand vous n'êtes pas connecté à Lastpass, et elle est colorée une fois que vous êtes connecté. Un clic dessus ouvre un menu qui vous demande votre login (e-mail) et votre mot de passe principal Lastpass (vous vous souvenez, celui que vous ne devez surtout pas oublier 😊).

Connexion à Lastpass

Lastpass vous propose de retenir votre e-mail. Vous pouvez laisser cette case cochée, c'est pratique.

En revanche, il vous propose de retenir votre mot de passe principal. C'est une TRÈS mauvaise idée pour la sécurité de votre compte. Ne cochez pas cette case. Si vous le faites, il vous dira que c'est une très mauvaise idée de toute façon.





N'oubliez pas que le mot de passe principal est l'élément qui déverrouille tous vos mots de passe. Il faut que vous fassiez l'effort de le saisir au moins une fois à chaque fois que vous allumez votre navigateur.

Une fois que vous êtes connecté, Lastpass synchronise tous vos mots de passe (cryptés) qu'il connaît. Si vous avez enregistré des mots de passe sur une autre machine, vous les retrouverez donc ici !



Pour information, les mots de passe sont stockés de façon cryptée sur les serveurs de Lastpass. La technique employée est réellement robuste : l'équipe de Lastpass ne peut pas lire vos mots de passe, il n'y a que votre mot de passe principal que vous seul connaissez qui permet de les décrypter.

Découvrir Lastpass

Si vous cliquez sur l'icône colorée de Lastpass, le menu s'ouvre :



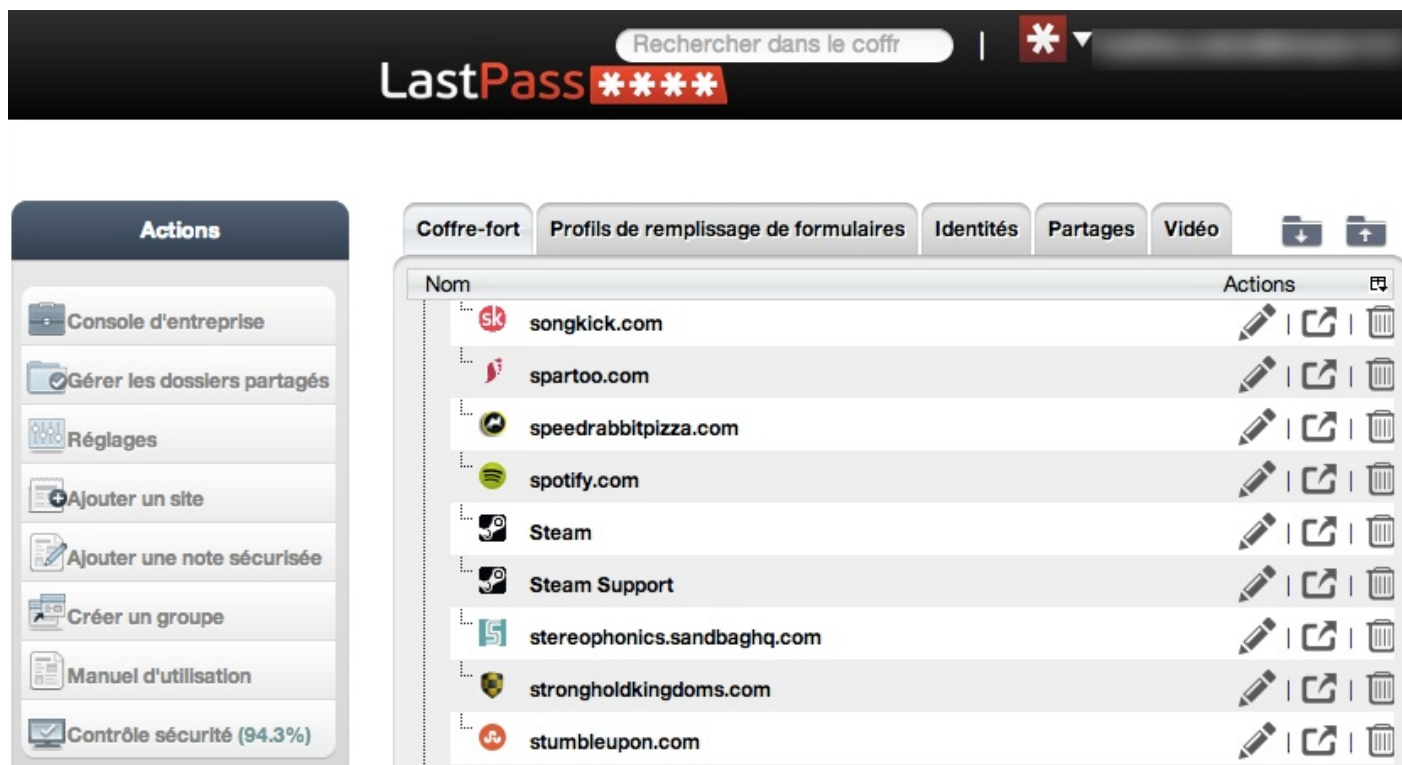
Menu principal de Lastpass

J'ai encadré en rouge les fonctionnalités que j'utilise le plus souvent en pratique :

- **Mon coffre-fort Lastpass** : affiche une fenêtre qui résume la liste des sites et des mots de passe enregistrés dans Lastpass
- **Notes sécurisées** : c'est un petit bloc-notes qui vous permet de saisir du texte qui sera crypté en même temps que vos mots de passe. Si vous avez des informations confidentielles dont vous voulez vous souvenir, vous pouvez utiliser ce menu pour en ajouter.
- **Remplir les formulaires** : vous permet de saisir des informations personnelles (comme votre adresse personnelle, ou même votre numéro de carte bleue) pour que Lastpass puisse les remplir automatiquement pour vous lorsque vous arrivez sur un nouveau site (par exemple un site e-commerce). C'est très pratique, je l'utilise, mais vu l'importance des informations j'active une double sécurité en demandant à Lastpass de me redemander mon mot de passe principal à chaque fois que je veux remplir des formulaires.
- **Générer un mot de passe sécurisé** : vous permet de générer des mots de passe sécurisés et complexes pour les sites que vous visitez. C'est là que Lastpass est génial : il vous aide à créer de multiples mots de passe très complexes... que vous n'aurez pas besoin de retenir, puisqu'il les retient pour vous ! Rappelez-vous : la seule chose que vous avez besoin de

retenir, c'est votre mot de passe principal.

Un clic sur "Mon coffre-fort Lastpass" ouvre une fenêtre qui ressemble à ceci (une fois que vous avez plein de mots de passe dedans 🤪) :



Le coffre-fort Lastpass contenant tous vos mots de passe

Vous pouvez à partir de là les modifier, les partager de façon sécurisée à des amis ou les supprimer (via les icônes sur la droite).

Enregistrer un nouveau mot de passe sur Lastpass

Bon concrètement, comment on fait pour enregistrer un nouveau mot de passe sur Lastpass ? On va prendre un exemple concret. On va aller créer un compte sur un site.

On tombe en général sur un formulaire comme celui-ci :

Les champs marqués par un astérisque * sont obligatoires.

* Nom d'utilisateur	: <input type="text" value="mateo21"/>	Caractères autorisés : a-z, 0-9,
* Mot de passe	: <input type="password"/>	6 caractères minimum. La casse
* Confirmer le mot de passe	: <input type="password"/>	
* Email	: <input type="text" value="moi@email.com"/>	
* Prénom	: <input type="text" value="Mathieu"/>	
* Nom	: <input type="text" value="Nebra"/>	
Date de naissance	: <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/>	
* Pays	: <input type="text" value="France"/>	

Un formulaire d'inscription

Vous remplissez les informations demandées comme d'habitude. Par contre, cette fois, vous n'aurez pas besoin de vous créer un mot de passe vous-mêmes : vous allez laisser Lastpass le faire pour vous ! 😊

Normalement, une barre apparaît en haut de votre navigateur, vous proposant de générer un mot de passe. Mais vous pouvez aussi aller dans le menu Lastpass en cliquant sur l'icône Lastpass, puis en sélectionnant "Générer un mot de passe sécurisé". Une fenêtre apparaît alors pour vous proposer des mots de passe complexes :



Le générateur de mots de passe

A vous d'indiquer la longueur que vous voulez pour votre mot de passe. N'hésitez pas à choisir quelque chose de long, vous n'avez pas besoin de le retenir et plus c'est long mieux c'est sécurisé ! Personnellement, quand les sites l'acceptent, j'essaie de mettre au moins 16 caractères et je demande à ce que Lastpass utilise des majuscules/minuscules/chiffres/caractères spéciaux. Ça fait des mots de passe très solides !

Vous pouvez cliquer sur "Générer" autant de fois que vous voulez, mais en général le premier mot de passe proposé sera tout aussi bien que les suivants. Vous pouvez à partir de là le copier et le coller dans le champ "Mot de passe" du formulaire (Lastpass peut aussi le remplir pour vous).

Validez ensuite le formulaire d'inscription du site. Lastpass vous propose alors de retenir votre identifiant et votre mot de passe :



Lastpass vous propose d'enregistrer les informations

Dites oui ! 😊

Cliquez sur "Enregistrer site". Une fenêtre apparaît pour vous permettre de confirmer :

The image shows the LastPass web interface for editing a password entry. At the top is the LastPass logo with four asterisks. Below it are input fields for 'URL' (http://www.ultimate-guitar.com/), 'Nom' (ultimate-guitar.com), 'Groupe' (Perso), 'Nom d'utilisateur' (mateo21), and 'Mot de passe' (masked with dots). A strength indicator bar is visible below the password field. There is an '[Afficher]' button next to the password field. A large 'Notes' text area is below the password field. At the bottom, there are four checkboxes: 'Favoris', 'Nécessite la re-saisie du mot de passe', 'Ne jamais remplir automatiquement', and 'AutoConnexion'. Two buttons, 'Enregistrer' and 'Annuler', are at the bottom right.

Modifier les informations sur le mot de passe avant de l'enregistrer

En général, je n'ai pas besoin de changer grand chose dans cette fenêtre, si ce n'est le groupe. Je classe mes mots de passe dans deux groupes : "Perso" et "Pro", ce qui me permet de mieux les distinguer.

Il y a des options en bas qui peuvent être intéressantes :

- **Favoris** : si vous voulez que le mot de passe fasse partie de vos favoris et apparaisse en haut de votre coffre-fort. Je l'utilise assez peu.
- **Ne jamais remplir automatiquement** : si vous ne voulez pas que Lastpass remplisse les formulaires pour vous avec ce mot de passe. Je n'en ai jamais vu l'intérêt.
- **Nécessite la re-saisie du mot de passe** : très pratique pour les mots de passe les plus sensibles (comme le site de votre banque, de paypal...). Il faudra re-saisir votre mot de passe principal pour déverrouiller ce mot de passe. C'est une sécurité supplémentaire mais je ne le fais pas pour tous les sites car ça peut vite devenir fatigant.
- **AutoConnexion** : Lastpass peut vous connecter automatiquement au site. Par défaut, il remplit juste le formulaire et vous laisse cliquer sur le bouton "Connexion", mais si vous êtes vraiment fainéants vous pouvez demander à Lastpass de cliquer sur "Connexion" pour vous pour aller plus vite. 😊

Une fois que vous avez cliqué sur "Enregistrer", c'est fini ! Le mot de passe sera crypté et synchronisé sur tous les autres ordinateurs où vous utilisez Lastpass !

Quand la magie opère : Lastpass remplit les champs de connexion pour vous !

C'est maintenant que les choses deviennent intéressantes. La prochaine fois que vous vous rendez sur le site où vous avez enregistré le mot de passe via Lastpass, il devrait automatiquement remplir l'identifiant et le mot de passe !

Sign in to your account

Your email address

contact@simple-it.fr



Your password

[Forgot password?](#)

.....



☐ Remember me for 2 weeks

GET AN ACCOUNT

Sign up now to see where your visitors are clicking.

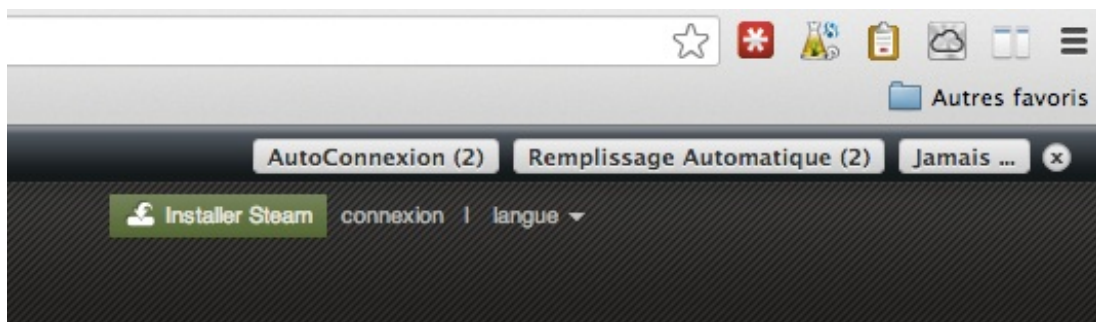
[View plans and pricing](#)

LOG IN

Lastpass remplit tout seul les champs du formulaire !

Vous reconnaissez la petite icône Lastpass dans le champ de formulaire qui indique que c'est Lastpass qui a pré-rempli le formulaire. Vous n'avez plus qu'à cliquer sur "Connexion" !

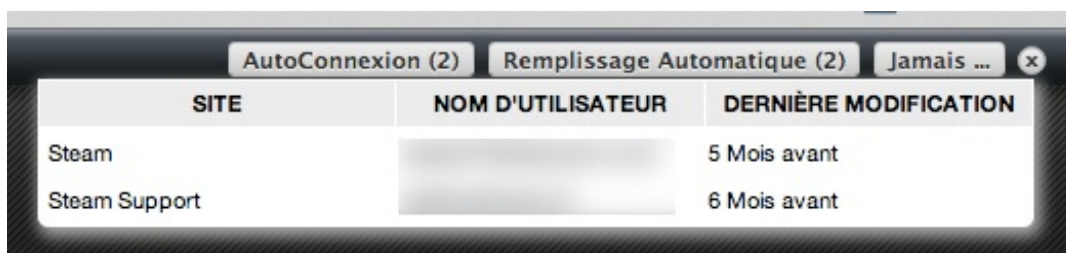
Parfois, vous aurez plusieurs comptes sur un même site web. Dans ce cas de figure, Lastpass affiche une barre pour vous proposer de choisir le compte que vous voulez utiliser :



Si vous avez plusieurs

comptes sur le site, une barre apparaît

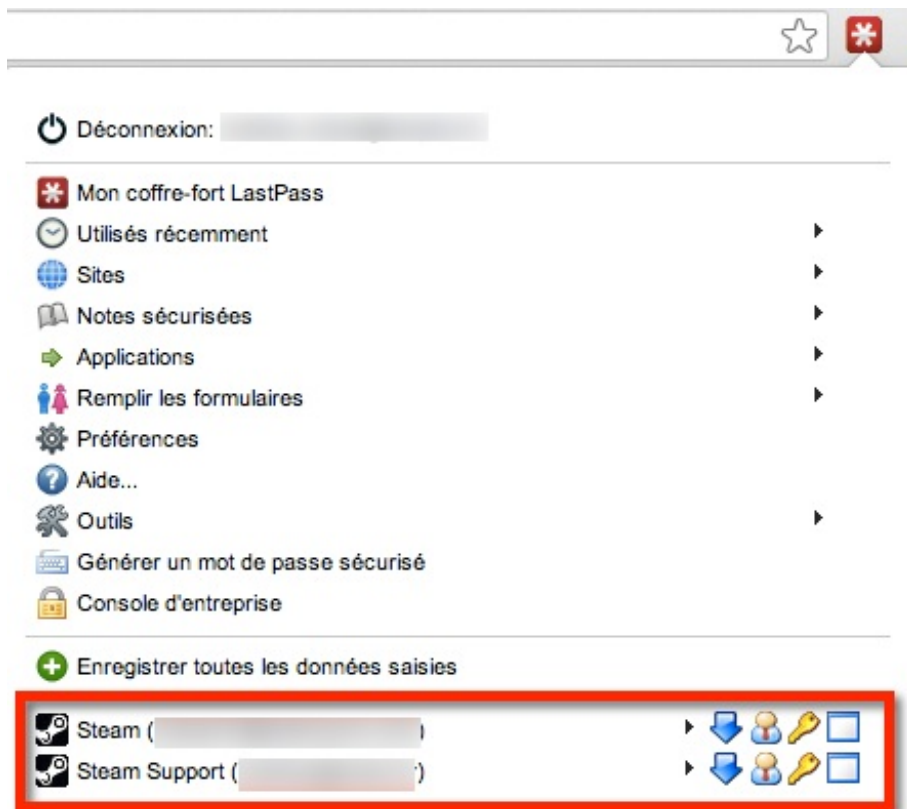
En général, je clique sur "Remplissage automatique" pour sélectionner le compte à utiliser :



Vous pouvez sélectionner le

compte que vous voulez utiliser

Quand vous êtes en train de visiter un site, vous pouvez aussi retrouver tous les mots de passe que connaît Lastpass pour ce site en cliquant sur l'icône pour afficher le menu. En bas du menu, vous voyez la liste des comptes enregistrés *pour le site que vous visitez* :



Vous pouvez aussi retrouver les mots de

passse du site que vous visitez dans le menu Lastpass

Les petites icônes à droite vous permettent respectivement de :

- Remplir le formulaire (la flèche vers le bas)
- Copier l'identifiant dans le presse-papiers (le bonhomme). Pratique quand le remplissage automatique du formulaire ne fonctionne pas, ce qui arrive des fois hélas.
- Copier le mot de passe dans le presse-papiers (la clé). Là encore pratique quand le remplissage automatique du formulaire ne fonctionne pas.
- Copier l'URL du site (la fenêtre). Ca je n'ai jamais eu besoin de l'utiliser par contre !

Améliorer la sécurité avec la double authentification

Comme vous l'avez vu, Lastpass est vraiment pratique. Un mot de passe vous permet de déverrouiller tous vos mots de passe !

Ceci étant, je recommande vraiment d'utiliser un système de double authentification. Cela implique, pour déverrouiller vos mots de passe :

- Que vous donniez quelque chose que vous *connaissez* (le mot de passe principal Lastpass).
- Que vous donniez quelque chose que vous *possédez* (comme une clé spéciale que vous transportez sur vous). Pour ça, vous pouvez soit :
 - Utiliser une **Yubikey** que vous accrochez à votre porte-clés. Seul problème : il faut acheter une Yubikey. Personnellement c'est ce que j'utilise, j'en ai acheté une sur Internet.
 - Utiliser l'application smartphone **Google Authenticator**. Elle génère des codes sécurisés qui changent dans le temps.

La Yubikey

Pour information, voici à quoi ressemble ma Yubikey au milieu de mon porte-clés :



Ma

Yubikey accrochée à mon porte-clés

Cette clé s'insère dans un port USB de l'ordinateur. En appuyant sur le bouton, elle génère un mot de passe unique (qu'elle seule connaît) et vous permet de remplir un champ à la connexion à Lastpass :

Authentification multi-facteurs Yubikey



1. Insérez votre YubiKey dans le port USB, la face avec le logo USB vers le haut.
2. Veuillez attendre que votre témoin lumineux YubiKey soit allumé en continu
3. Maintenez votre doigt sur le bouton pendant 2 secondes

 |

☒ Cet ordinateur est fiable, ne nécessitant pas une seconde authentification.
Merci de donner un nom à cet ordinateur

[Si vous avez perdu votre YubiKey, cliquez ici pour désactiver l'authentification par YubiKey](#)

La fenêtre qui demande d'insérer la Yubikey pour se connecter à Lastpass

En clair, c'est un second mot de passe (en plus du mot de passe principal) qu'on vous demande de saisir pour que la connexion à Lastpass soit autorisée. Vous n'avez pas besoin de retenir ce mot de passe car il change tout le temps (à chaque connexion !),

c'est votre Yubikey qui la connaît.



Pour information j'ai appris récemment que tous les employés de Google avaient eux aussi une Yubikey pour pouvoir faire de la double authentification pour accéder à leurs services internes ! 😊

Le défaut de la Yubikey, c'est qu'il faut acheter un compte Lastpass premium (12\$ par an, pas très cher ceci dit) pour pouvoir l'utiliser... et il faut acheter la Yubikey en ligne auprès de [Yubico](#).

Je ne pense pas que c'est ce que la plupart d'entre vous feront... Voilà donc pourquoi je vous propose plutôt d'utiliser l'authentification via Google Authenticator.

Google Authenticator

Google Authenticator est une application Android & iPhone créée à la base par Google pour sécuriser les accès à Gmail avec de la double authentification. Aujourd'hui, de nombreux services se basent dessus pour faire eux aussi de la double authentification (Dropbox par exemple).

Pour utiliser Google Authenticator, vous devez disposer d'un smartphone (logique 📱). L'application est gratuite.


Rendez-vous ensuite dans votre coffre-fort Lastpass et cliquez à gauche sur le menu "Réglages". Une fenêtre apparaît, qui vous donne accès à des réglages avancés.

Rendez-vous sur l'onglet "Multifactor options" et sélectionnez "Google authenticator". On vous propose de scanner un QR Code : utilisez votre smartphone depuis l'application Google Authenticator pour le faire. Cela liera Lastpass avec votre smartphone.

Modifier les paramètres

Général Sécurité Domaines équivalents URLs exclues **Multifactor Options** Périphériques mobiles Ordinateurs de confiance Règles d'URL


Choose a multifactor option: ☐ YubiKey ☒ Google Authenticator

 LastPass peut être configuré pour fonctionner avec Google Authenticator. Google Authenticator est un service sécurisé, facile à utiliser, d'authentification à deux facteurs pour votre appareil mobile qui vous protège d'attaques par relecture, d'attaques d'homme-au-milieu, et d'une foule d'autres vecteurs de menaces.

L'authenticator Google rend LastPass plus sûr et plus facile à utiliser.

Pour installer l'application Google Authenticator sur votre appareil mobile, visitez le site [GOOGLE AUTHENTICATOR!](#)

Pour associer l'authentificateur avec votre compte Google, scanner le code barre ci-dessous avec votre demande Google Authenticator.



[Cliquez ici si vous êtes incapable de scanner le code barre \(par exemple si vous utilisez l'application BlackBerry, ou un dispositif sans caméra\).](#)

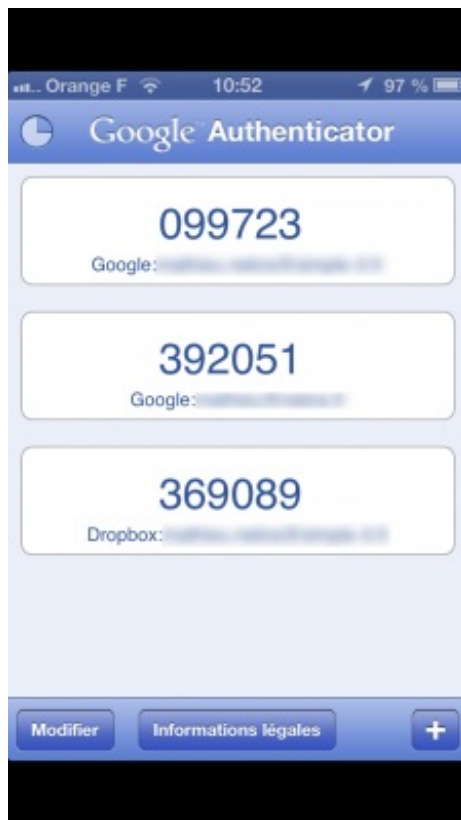
Authentification Google Authenticateur Aide...

Permettre l'accès hors ligne Aide...

[Click here to regenerate your Google Authenticator key \(for example if you lost your Google Authenticator device\).](#)

Configuration de Google Authenticator

Et voilà ! Désormais, votre smartphone génère des mots de passe à 6 chiffres qui changent régulièrement ! Voici pour information à quoi ressemble l'application quand elle me génère des mots de passe :



L'application Google Authenticator

Lors de la connexion à Lastpass, on vous demandera de saisir le code à 6 chiffres que vous voyez en ce moment sur l'application Google Authenticator.

Avec ça vous êtes prêts ! Pour que quelqu'un vole vos mots de passe, il doit connaître votre mot de passe principal Lastpass *et* vous assommer dans la rue pour récupérer votre smartphone ! 😊

Partager

