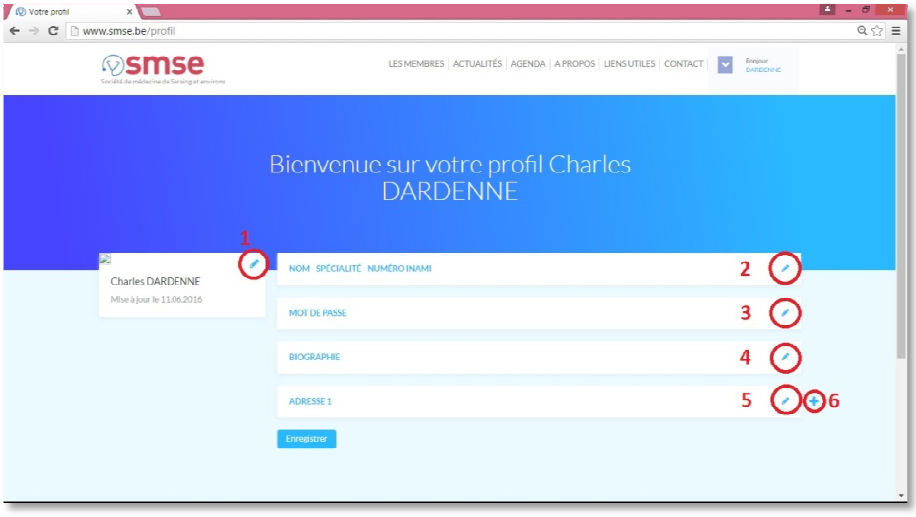
Procédure de modification du mot de passe

Procédure de modification d'un mot de passe.

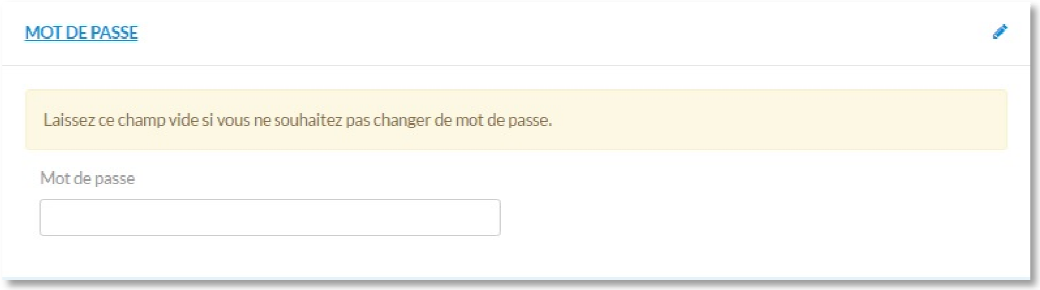
1. Vous venez de récupérer un nouveau mot de passe. Celui-ci vous parait difficile à retenir alors changer le !
2. Loguez-vous sur le site avec votre login (adresse mail) et votre mot de passe. Si ces deux informations sont correctes, vous arrivez sur le site avec en haut à droite votre nom.

3. Ouvrez le menu déroulant à l'aide de la petite flèche bleue dirigée vers le bas (en fonction de la résolution de votre écran, la présentation de ce menu peut être différente) et sélectionnez – Mon profil –

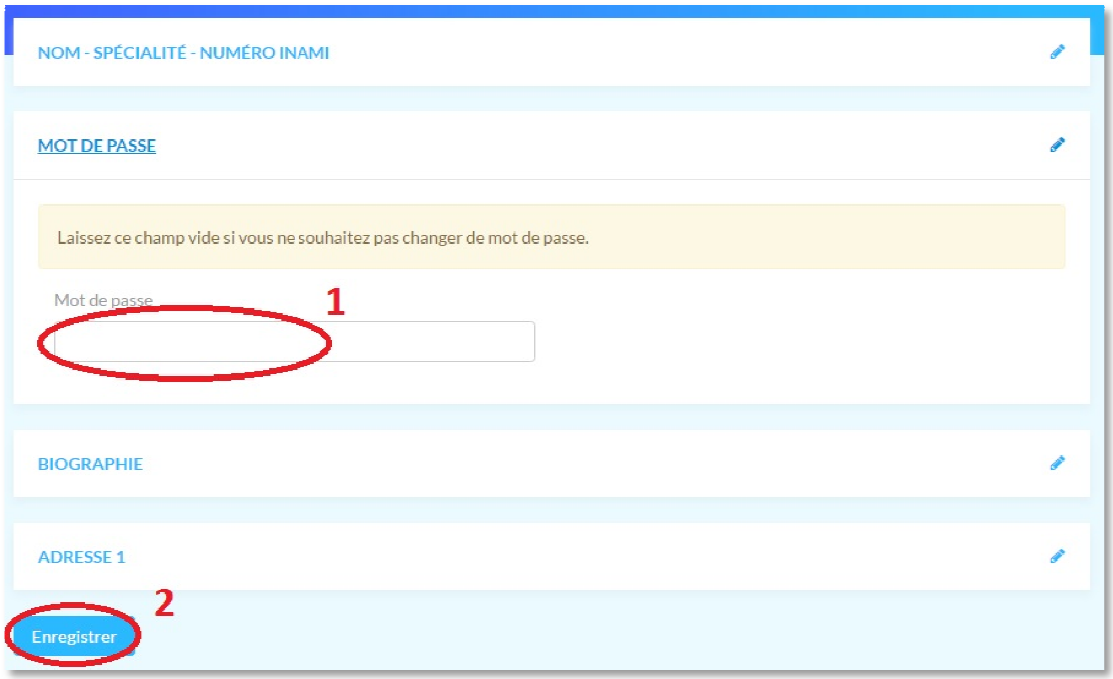
4. Vous entrez alors dans votre profil complet. Le changement du mot de passe se fait au niveau du point n°3. Cliquez sur le crayon !



5. Tapez votre nouveau mot de passe dans le champ. (ATTENTION à respecter les majuscules-minuscules)



6. Et SURTOUT enregistrez votre modification.



7. Votre nouveau mot de passe est à présent actif.

ADDENDA : comment choisir un bon mot de passe ?

1. problème

De nos jours, on utilise beaucoup de mots de passe pour accéder à nos mails, chatter, accéder à nos fichiers, régler nos factures... pas évident de tout retenir.

- Certains on tendance à utiliser **le même mot de passe partout**. C'est une très mauvaise idée: Si un pirate parvient à trouver votre mot de passe, il aura accès à tout ! C'est trop **dangereux**.
- Quand on prend des mots de passe différents, on a rapidement tendance à les **oublier**.
- Quand on choisit de mots de passe **trop simples** (plus faciles à retenir), il devient plus facile pour les hackers de les **deviner**.

- Certains laissent les **logiciels** retenir leurs mots de passe, ce qui est dangereux car le **piratage** est possible, et en cas de problème (plantage, réinstallation) vous **perdez** tous vos mots de passe.

Idéalement, un bon mot de passe est long (plus de 8 caractères) et mélange lettres, chiffres et symboles.
Alors comment choisir un mot de passe assez complexe mais facile à retenir ?

2. Une méthode efficace

Voici une méthode efficace:

- **Choisissez une phrase**
- **Prenez la première lettre de chaque mot**
- **Ajouter quelques chiffres et symboles.**

> Un exemple:
>
> - **L**a **g**rand-**m**ère **m**ange **l**es **p**issenlits **p**ar **l**a **r**acine
> - Ce qui donne: **Lgmmlpplr**
> - On ajoute chiffres et symboles: Lgmm**776**lpplr**&&**

De cette manière, le mot de passe est long et pratiquement inattaquable par les Attaques par Dictionnaire , et vous pourrez le retrouver assez facilement à partir de la phrase.

3. Un mot de passe différent pour chaque site

Il ne faut jamais utiliser le même mot de passe sur différents sites.

Il y a moyen, à partir de la méthode précédente, d'avoir un mot de passe différent pour chaque site: Vous pouvez utiliser une phrase en rapport avec le site, par exemple: "*J'adore mon Canon EOS 300D*" sur Flickr.com, "*A mort les spammeurs*" sur GMail.com, etc.

Autre solution: utiliser une partie du nom de domaine dans votre mot de passe.

Par exemple, si votre mot de passe est Lgmm776lpplr&&, utilisez:

- Lgm**f**776lpplr&& sur **f**lickr.com
- Lgm**c**776lpplr&& sur **c**ommentcamarche.net
- etc.

(Ou toute autre partie du nom de domaine: les deux avant-dernières lettre, etc. Vous avez le choix.)

Ainsi:

- Cela vous fait seulement un mot de passe (une phrase) à retenir (Le mot de passe spécifique au site peut se déduire du nom du site)
- Si un webmaster mal intentionné a votre mot de passe, il ne pourra pas facilement deviner le mot de passe des autres sites.

NB : sur notre site web, votre mot de passe n'est pas stocké en clair. Cela veut dire qu'il n'est pas possible pour le webmaster d'accéder à votre mot de passe.

Il s'agit ici d'un respect déontologique de développeur de crypter les mots de passe.

C'est pour cette raison que lors du renvoi de votre mot de passe, le système génère un nouveau mot de passe. Il est incapable de vous renvoyer votre mot de passe initial.

Pou ceux que cela intéressent, notre chiffrement utilise le cryptage, la hashage, le salt et donne un niveau de sécurité optimal.