Comment créer un mot de passe fort et sécurisé ?

1. Les règles à respecter pour créer un bon mot de passe

Règle n°1 : 12 caractères

Un mot de passe sécurisé doit comporter au moins **12 caractères**. Il peut être éventuellement plus court si le compte propose des sécurités complémentaires comme le verrouillage du compte après plusieurs échecs, un test de reconnaissance de caractères ou d'images («captcha») etc...

Règle n°2 : des chiffres, des lettres, des caractères spéciaux

Votre mot de passe doit se composer de **4 types de caractères différents** : majuscules, minuscules, chiffres, et signes de ponctuation ou caractères spéciaux (€, #...)

Règle n°3 : un mot de passe anonyme

Votre mot de passe doit être **anonyme** : il est très risqué d'utiliser un mot de passe avec votre date de naissance, le nom de votre chien etc., car il serait facilement devinable ; en **mot de passe fort** ne doit pas comporter :

- vos informations personnelles faciles à trouver : nom, prénom, date de naissance
- mots évidents, expressions courantes, suites ou répétitions de caractères ; par exemple, motdepasse, password, azerty, 1111, 1234567.

Règle n°4 : la double authentification

Certains sites proposent de vous **informer par mail ou par téléphone** si quelqu'un se connecte à votre compte depuis un terminal nouveau. Vous pouvez ainsi accepter ou refuser la connexion. N'hésitez pas à utiliser cette option. (sécurité bancaire par exemple)

Règle n°5 : renouvellement des mots de passe

Sur les sites où vous avez stocké des données sensibles, pensez à **changer votre mot de passe régulièrement** : tous les 3 mois parait être une fréquence raisonnable.

2. Comment retenir son mot de passe ?

Il est très important d'**utiliser un mot de passe différent pour chaque compte**. Vous devez donc construire plusieurs mots de passe, et pas question de les écrire dans un fichier texte, dans les notes de votre smartphone ou sur le cloud : ils pourraient être facilement consultables. Alors, comment les retenir ?

La **Commission nationale de l'informatique et des libertés (CNIL)** a mis en place un **générateur de mots de passe** qui permet de créer son mot de passe à partir d'une phrase. Vous n'avez qu'à retenir la phrase et utiliser les initiales de la phrase pour créer votre mot de passe.

https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

3. Quels risques à utiliser un même mot de passe pour plusieurs sites ?

Si un des sites sur lesquels vous avez un compte est victime de fuite de données comprenant vos moyens d'authentification, il sera alors facile pour les pirates d'**accéder à vos informations personnelles**. Ils pourraient utiliser vos identifiants et mots de passe pour se connecter à d'autres comptes. Soyez très vigilants, et surtout sur des comptes qui comportent des **données sensibles** (réseaux sociaux, boîte mail etc.).

Par exemple, s'il contrôle l'accès à vos comptes sur internet, un pirate pourrait :

- usurper votre boîte mail pour **piéger vos contacts**
- **utiliser vos données bancaires** pour des **achats frauduleux**
- **usurper votre identité**
- **demander une rançon** s'il trouve des données compromettantes dans votre boîte mail

4. En cas d'oubli de mot de passe

En cas d'oubli de votre mot de passe, vous avez la possibilité d'en créer un nouveau.

Pour cela, où que vous soyez (valable sur n'importe quel site)

- cliquez sur « mot de passe oublié »
- saisissez votre adresse électronique d'inscription ; vous allez recevoir par retour de mail ou par sms un code d'identifiant (ou un mot de passe temporaire)
- vous pourrez ainsi vous reconnecter et générer un nouveau mot de passe.

Fait par Françoise

http://synapse91.com