CYBERNADETTE

Atelier numérique dédié aux jeunes de soixante ans et plus

Aide mémo pour bien créer et gérer ces mots de passe !

Pourquoi et comment bien gérer ses mots de passe ?

Messageries, réseaux sociaux, banques, administrations et commerces en ligne… La sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple.
Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. On vous dit tout en 10 points !

1 - Utilisez un mot de passe différent pour chaque service
Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

2 - Utilisez un mot de passe suffisamment long et complexe
Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux et ne ressemble en aucun cas à un mot commun ou mot propre.
> Ex de mot de passe complexe crée : Z14h+mP8bak55

3 - Utilisez un mot de passe impossible à deviner
Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré.
Évitez également les suites logiques simples comme 123456, azerty … qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

Comment créer un mot de passe solide ?

La méthode des premières lettres **:** *Un tiens vaut mieux que deux tu l'auras* **:**
1tvmQ2tl'A

La méthode phonétique ***:*** *J'ai acheté huit CD pour cent euros cet après-midi* **:**
ght8CD%E7am

4 - Utilisez un gestionnaire de mots de passe
Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ni dans votre Smartphone auquel un cybercriminel pourrait avoir accès. Identifier un carnet qui sera destiné uniquement à y écrire le mot de passe et le compte qui s'y rattache

5 - Changez votre mot de passe au moindre soupçon

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

6 - Ne communiquez jamais vos mots de passe à un tiers

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

7 - N'utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un cybercriminel.
Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez aussi à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur en automatique.

8 - Activez la double authentification (*Également appelée "authentification forte")* **lorsque c'est possible**

Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail). Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés.

9 - Changez les mots de passe par défaut des différents services auxquels vous accédez

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

10 - Choisissez un mot de passe particulièrement robuste pour votre messagerie

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction "mot de passe oublié" des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.
Votre mot de passe de messagerie est donc l'un des plus importants à protéger !

Pour aller plus loin :

– Par la CNIL : **Les conseils pour un bon mot de passe**
– Par l'ANSSI **: La sécurité des mots de passe**