La gestion des mots de passe

Les spécialistes en cybersécurité sont unanimes : les humains représentent le maillon faible dans la chaîne de sécurité en informatique. Une des principales failles en sécurité est l'utilisation d'un mot de passe trop simpliste. Pour vous aider à assurer une meilleure sécurité de vos comptes, voici quelques conseils…

Créer un mot de passe complexe

Plusieurs sites web le recommandent : votre mot de passe doit contenir au minimum 8 caractères, associant majuscules, minuscules, chiffres et caractères spéciaux.

La CNIL met à votre disposition un générateur de mot de passe particulièrement efficace, élaboré à partir d'une phrase de votre choix : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide .

Créer plusieurs mots de passe

Utiliser le même mot de passe pour différents sites web est une erreur régulière. En effet, si une personne malintentionnée parvient à récupérer le mot de passe de votre compte Facebook, elle pourra avec ce même mot de passe se connecter sur votre messagerie, sur votre compte ameli, sur votre compte impots.gouv.fr ou encore sur votre compte bancaire…

Diversifiez donc vos mots de passe. A chaque site, un nouveau mot de passe !

Comment faire pour les mémoriser ? Trois astuces s'offrent à vous.

1 – Elaborez une combinaison. Attribuez par exemple la première lettre du site sur lequel vous vous inscrivez à votre mot de passe, saisissez ensuite vos lettres, vos chiffres et caractères spéciaux.

Ex : Sur Facebook, saisissez un mot de passe de type « FRegB$35h ». Sur Gmail, saisissez un mot de passe de type « GRegB$35h ». Sur Twitter, saisissez un mot de passe de type « TRegB$35h »…

Vous obtiendrez ainsi un mot de passe différent d'un site à l'autre, mais avec une combinaison simple à mémoriser. Cette méthode retardera l'intru quelques temps pour passer d'un site à l'autre mais nécessitera en revanche de modifier tous vos mots de passe au plus vite en cas de piratage.

2 – Notez vos mots de passe dans un carnet. Sans doute l'une des solutions les plus simples mais soyez particulièrement vigilants à ne pas égarer votre carnet ! Ne le laissez pas non plus à proximité de votre ordinateur : en cas de vol, votre agresseur pourrait à la fois repartir avec votre ordinateur et les mots de passe associés. Placez si possible votre carnet dans un endroit fermé sous clé.

3 – Utilisez un générateur de mots de passe. Cette méthode est l'une des plus sécurisées. Des logiciels tels que Keepass peuvent générer des mots de passe cryptés à votre place. L'utilisation d'un tel outil nécessite en revanche de mémoriser un seul mot de passe : celui de votre compte administrateur Keepass !

Pour plus d'informations, n'hésitez pas à consulter la page dédiée aux mots de passe de la CNIL : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe