MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

14 octobre 2024

ALERTECYBERGEND

Dans le cadre du Cybermoi/s 2024 et de la campagne nationale « Fausse Bonne Idée », le groupement de gendarmerie départementale de la Somme vous invite à rejoindre le mouvement pour une meilleure cybersécurité.

Le sujet du jour : le rôle crucial des mots de passe dans notre monde hyperconnecté.

L'IMPORTANCE DES MOTS DE PASSE

Au cœur de la cybersécurité d'une entreprise, d'une collectivité ou d'un particulier, se trouve la gestion des mots de passe. De nombreuses attaques sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre. Le risque est d'autant plus grand qu'une attaque réussie sur un seul compte peut entraîner une propagation de logiciels malveillants à l'échelle de l'entreprise, voire au-delà, en exploitant les contacts de la victime pour mener de nouvelles attaques.

QUELLES DOIVENT ÊTRE LES CARACTÉRISTIQUES D'UN MOT DE PASSE ?

- **Unique** : chaque compte en ligne devrait avoir un mot de passe unique. Évitez de réutiliser le même mot de passe sur différents sites. Si un de vos comptes est compromis, seul ce compte est en danger. Le pirate n'aura pas les clés pour accéder aux autres.

- **Robuste** : pour renforcer votre sécurité en ligne, privilégiez des mots de passe longs et complexes (au minimum 9 caractères pour les services non critiques, et 14 pour les services critiques), composés d'un mélange de majuscules, minuscules, chiffres et symboles, et évitez les mots courants ou les informations personnelles facilement accessibles. Enfin, activez la « double authentification » lorsque c'est possible.

- **Mémorisable** : cela va sans dire… Bien que la complexité soit indispensable, le mot de passe doit pouvoir être retenu facilement.

QUELQUES ASTUCES POUR MÉMORISER SES MOTS DE PASSE

Le post-it (comme tout support physique) n'est pas le meilleur endroit pour conserver vos mots de passe, loin s'en faut. Explorons ensemble quelques méthodes plus sûres pour les gérer :

➔ **La phrase de passe** (« **passphrase** » en anglais) : les phrases de passe consistent à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé (comme le dictionnaire de la langue française). Les passphrases sont souvent bien plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à retenir.

➔ **L'application de gestion de mots de passe** (également appelée « **coffre-fort** » à mots de passe) : ce type d'application peut vous aider à générer des mots de passe robustes et à ne pas avoir à les mémoriser. Elle permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe, qualifié « maître ». Parmi la diversité des applications disponibles, il est très largement conseillé d'utiliser un coffre-fort certifié par l'ANSSI (agence nationale de la sécurité des systèmes d'information).

En conclusion, la compromission d'un seul mot de passe peut avoir des conséquences bien plus larges que la simple perte d'un compte. Elle peut servir de point d'appui pour mener des attaques plus complexes et à plus grande échelle.

En investissant quelques minutes pour mettre en place une solution de gestion de mots de passe, vous protégez vos données et celles de vos proches ou de votre entreprise.