Pourquoi il ne faut pas enregistrer vos mots de passe dans les navigateurs

Par Patrick Sentinel – 29a.ca

Aujourd'hui, la tentation de laisser son navigateur enregistrer ses mots de passe est intéressante et alléchante! C'est rapide, très pratique, et ça évite de devoir se souvenir de cette longue série de caractères que vous avez créée pour chaque site. Pourtant, même si cela semble être une bonne idée, enregistrer ses mots de passe dans un navigateur est risqué. Voici pourquoi il vaut mieux éviter cette pratique!

Les risques de sécurité associés

1. Vulnérabilité aux attaques

Les navigateurs sont des cibles fréquentes pour les cybercriminels. Si un maliciel trouve son chemin dans votre appareil, il pourrait facilement accéder aux **informations enregistrées dans votre navigateur, y compris vos mots de passe**. Vous me direz probablement qu'en général les mots de passe sont hachés/chiffrés dans l'ordinateur. À moins de les vérifier un par un, vous n'en savez rien! De plus, le hachage/chiffrement pourrait être complètement désuet. Les pirates ont plus de patience que vous pour deviner des combinaisons de mots de passe; pourquoi leur faciliter la tâche ?

2. Accès non autorisé

Si une personne met la main sur votre appareil, il pourrait accéder à vos comptes **avec les mots de passe stockés dans votre navigateur**. Imaginez que vous laissiez les clés de votre maison sous le paillasson, tout en espérant pour que personne ne les trouve. C'est un peu l'idée ici… Mieux vaut ne pas courir ce risque, surtout si votre appareil est volé ou perdu.

3. Manque de protection avancée

Les navigateurs offrent un certain niveau de sécurité, mais **ils ne sont pas conçus pour gérer des informations aussi sensibles que vos mots de passe**. Utiliser un navigateur pour stocker vos mots de passe, c'est comme utiliser une boîte à biscuits pour cacher vos économies ou utiliser un parapluie troué sous la pluie! Ça peut marcher, mais ce n'est probablement pas la solution le plus sécurisé.

Les alternatives sécurisées

1. Gestionnaires de mots de passe

Les gestionnaires de mots de passe sont conçus spécifiquement pour stocker vos informations de manière sécurisée. Ils chiffrent vos mots de passe avec une méthode normalement approuvée par l'industrie et exigent une authentification forte pour y accéder. C'est un peu comme engager un garde du corps pour protéger vos informations personnelles. Vous ne confieriez pas cette tâche à votre chat, non?

2. Authentification à deux facteurs (2FA)

L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire à vos comptes en ligne. Même si un pirate réussit à obtenir votre mot de passe, il aura besoin d'une deuxième forme d'authentification pour accéder à votre compte. C'est comme une porte blindée derrière une autre porte blindée; deux fois plus de protection, deux fois moins de chances que quelqu'un entre sans permission. L'authentification à deux facteurs doit être activée sur **TOUS** vos comptes! C'est simple à activer et elle peut vous économiser beaucoup de soucis.

Conclusion

Enregistrer vos mots de passe dans un navigateur peut sembler pratique, mais les risques pour la sécurité de vos informations sont trop importants pour être ignorés. Utiliser un gestionnaire de mots de passe réputé et activer l'authentification à deux facteurs sont des mesures simples qui peuvent grandement améliorer votre cybersécurité. En fin de compte, mieux vaut prévenir que guérir; et surtout, mieux vaut ne pas confondre commodité avec sécurité.