27.01.2023

Suivez-vous les bonnes pratiques en matière de mots de passe ?

Les chercheurs en sécurité ne sont pas satisfaits du comportement des internautes en matière de mots de passe : malgré les campagnes de sensibilisation, une grande majorité des utilisateurs/trices continuent d'ignorer les règles de sécurité de base permettant de sécuriser leurs mots de passe.

« Les mots de passe les plus stupides de 2022 » : tel est le titre d'un article publié récemment dans le magazine informatique allemand PCtipp. Comme les années précédentes, la séquence de caractères « 123456 » occupe la première place du palmarès des mots de passe les plus populaires, un classement établi chaque année par l'Institut Hasso Plattner (HPI). Le reste du top 10 ne fait pas beaucoup mieux sur le plan de la sécurité. Résultat des courses : on estime à plus d'un million, le nombre de données de connexion piratées.

Plus un mot de passe est facile à retenir, plus il sera facile à pirater. Ainsi, un ordinateur standard mettra moins d'une minute pour hacker le fameux mot de passe « 123456 ».

Alors, pourquoi les campagnes d'information sur la bonne gestion des mots de passe sont-elles apparemment si peu efficaces ? Des études telles que la « Psychologie des mots de passe » réalisée par le fournisseur de gestionnaires de mots de passe LastPass tentent d'apporter des éléments de réponse à cette question. Selon cette étude, la très grande majorité des personnes interrogées était convaincue d'utiliser correctement leurs mots de passe et 73 % d'entre elles les considéraient même comme forts. Petite précision : si 69 % des répondants indiquent utiliser des mots de passe sûrs en e-banking, ils ne sont plus que 38 % à le faire pour les réseaux sociaux.

L'aspect générationnel joue également un rôle dans cette répartition. Les jeunes en particulier adoptent inconsciemment un comportement risqué en matière de mots de passe. Mais ce qui frappe, c'est qu'indépendamment de l'âge, les connaissances acquises lors des formations sur la sécurité ne sont pas, ou trop peu, mises en pratique.

Les gestionnaires de mots de passe tels que KeePass par exemple peuvent s'avérer utiles dans la mesure où ils facilitent énormément la gestion des identifiants d'accès, indépendamment de la solidité des mots de passe. Pour en savoir plus sur l'utilisation sécurisée des mots de passe, cliquez ici (https://www.ebas.ch/step4#mots%20de%20passe) .