Sécurité : des chercheurs favorables à la réutilisation des mots de passe

Selon une majorité d'experts en sécurité, **les mots de passe sont le talon d'Achille de la sécurité informatique**. Et les recommandations sont légions sur le fait de trouver des mots de passes complexes comprenant des minuscules, des majuscules et des caractères numériques ou spéciaux. La longueur de la chaîne de caractères est aussi importante pour compliquer la tâche de gens mal intentionnés. Un autre atout est de changer régulièrement ses mots de passe.

Cependant pour la plupart des personnes, il est quasi impossible de retenir plusieurs mots de passe complexes et de les changer régulièrement, à moins de se doter d'un gestionnaire d'identifiants ou d'un service cloud qui sauvegarde les mots de passe. Et encore **selon une étude**, ces outils ne seraient pas complétement sécurisés après la découverte récente de certaines vulnérabilités. Habituellement, les utilisateurs trouvent des mots de passe faciles : 123456, Azerty, password, sont devenus des références.

Réutiliser des mots de passe pour les comptes sans valeur

Et bien pour des chercheurs de Microsoft et l'Université Carleton, ce type de mot de passe n'est pas à écarter ou à considérer comme une mauvaise idée. *« Dans la pratique, de nombreux utilisateurs utilisent le même mot de passe pour un groupe de comptes. Mais il n'existe que peu d'indications sur le choix des groupes. Etant donné que la réutilisation des mots de passe se fera, nous étudions la manière de le faire plus intelligement »*, explique **Dinei Florencio** et **Cormac Herley** de Microsoft et **Paul C. van Oorschot** de l'Université Carleton au Canada dans le document « Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts »

L'étude montre que **l'usage de mot de passe complexe** doit être privilégié pour l**es sites considérés comme sensibles** ou importants tels que les services bancaires, les sites liés à la santé. La réutilisation d'un mot de passe simple sera affectée à des sites où les pertes potentielles de données jugées minimes par l'utilisateur. Les chercheurs soulignent que « *le rendement marginal de l'effort est inversement proportionnel à la valeur des comptes* ». Ils soutiennent donc que « *la réutilisation de mot de passe doit faire partie du portefeuille technique de sécurité, même si cela n'est pas la panacée* ». Les utilisateurs pourront alors se concentrer un peu plus pour chercher des mots de passe plus complexes pour les comptes sensibles.

A lire aussi :

Google veut mettre fin aux mots de passe