Les mots de passe longs et complexes sur le web ne sont plus ni utiles ni efficaces

Longtemps recommandés comme étant le graal de la sécurité, les mots de passe longs et complexes sont devenus aujourd'hui désuets. En cause les récentes fuites des géants du web, à la suite desquelles de nombreux mots de passe, aussi compliqués soient-ils, se sont retrouvés sur le net, à la vue de tous. On t'explique comment protéger tes données désormais.

Pour ta boîte mail, pour Facebook, Twitter, Instagram, LinkedIn, Skype, Netflix, ou encore pour accéder à ton iCloud, c'est un classique : tu as dû inventer un mot de passe le plus complexe possible au moment de configurer ton compte. Parfois ces services requièrent plusieurs caractères, dont au moins une majuscule, des chiffres et des lettres. Résultat : lorsque tu dois te reconnecter, tu ne parviens plus à te souvenir de ton mot de passe.

Or, ces mots de passe fastidieux ne sont aujourd'hui plus du tout efficaces. "Le conseil de sécurité que vous avez toujours entendu, à savoir d'avoir un mot de passe long et complexe, composé de majuscules, de symboles, de chiffres et de ponctuation, tout cela n'a plus d'importance", affirme ainsi à L'Écho Mark Risher, directeur sécurité et confidentialité chez Google. "Car en cas de violation sur un site en particulier, de par la propagation dans le domaine public de ces données à un moment donné, cette couche de protection tombe partout au final", poursuit-il.

Plus de 3 milliards de mots de passe publics sur le web

Et de fait, "nous avons trouvé plus de 3 milliards de noms d'utilisateurs et mots de passe en quelques semaines à peine, sur le web public uniquement", déplore-t-il. Le problème, c'est que "17 % des mots de passe choisis par les utilisateurs sont réutilisés entre différents sites internet", cite-t-il sur base d'une étude réalisée par Google. Ce qui rend donc totalement "obsolètes" les mots de passe longs et compliqués puisque ces codes se retrouvent, au final en cas de fuite, à la vue de tous sur le web.

Et une fois que tes données personnelles figurent dans ces "credential dumps" (ou puits de données), tu t'exposes "à 10 fois plus de tentatives de violation que la normale", avertit Risher. Ce qui fait de toi une cible facile de fishing (ou hameçonnage), cette nouvelle technique de hack qui consiste à te faire croire que tu t'adresses à un tiers de confiance (banque, commune, opérateur téléphonique, etc.) pour te soutirer des renseignements personnels (mots de passe, numéros de cartes bancaires, dates de naissance, numéros de registre national, etc.).

Que faire ?

Tu l'auras compris, mieux vaut mettre toutes les chances de ton côté pour empêcher tes mots de passe de fuiter sur le net. Et comment ? Le "Monsieur mot de passe" de Google recommande d'opter pour des mots de passe générés aléatoirement et qui sont donc uniques et différents pour tous tes comptes Google, Gmail, Facebook, Twitter, Instagram, etc. Pour ne pas t'embrouiller dans tous tes codes, tu peux utiliser un gestionnaire de mots de passe, soit un logiciel crypté qui conserve tous tes mots de passe dans un seul et même lieu, en sécurité maximale. Tu as le choix par exemple entre Dahslane, 1pass, LastPass ou encore 1Password.

Les géants du web ont évidemment leur part de responsabilité. Les bons élèves utilisent notamment la double authentification, qui consiste par exemple à t'envoyer un code secret par SMS pour te connecter sur leur système, et qui assure donc une meilleure sécurité de tes données. Mais pour les autres, il faudra le plus souvent guérir que prévenir...

On l'a d'ailleurs constaté ces derniers mois avec le scandale Cambridge Analytica, qui a exposé quelque 87 millions de comptes Facebook, dont 61.000 en Belgique, ou avec le dernier piratage du réseau social en septembre, qui a affecté 50 millions de comptes, ou encore, chez Google cette fois,

avec la faille informatique qui a rendu public durant trois ans les données personnelles d'un demi-million de comptes Google+. Il ne faut donc pas compter dessus : les géants du web ne sont plus en mesure d'assurer la sécurité des comptes de leurs utilisateurs ainsi que la protection de leurs données privées.

https://www.msn.com/fr-be/actualite/technologie-et-sciences/voil%c3%a0-pourquoi-les-mots-de-passe-longs-et-complexes-sur-le-web-ne-sont-plus-ni-utiles-ni-efficaces/ar-BBOgXfQ?li=BBqiJuZ&ocid=mailsignout