Les ondes cérébrales pour remplacer les mots de passe ?

Le cerveau est le terrain de jeu favori des chercheurs dans plusieurs directions : création de puces, mémoires récréant des réseaux neuronaux, étude sur le deep learning, etc. Dans la même veine, des universitaires de l'Université de Binghamton aux Etats-Unis ont mené des travaux qui pourraient bien redistribuer la donne en matière d'authentification ou de gestion des mots de passe.

L'étude 'Brainprint' a été réalisée sur **45 volontaires**. Ils ont lu **75 acronymes comme DVD ou FBI**. Pendant leur lecture, leur activité cérébrale a été enregistrée et analysée en se concentrant sur la partie du cerveau associée à la lecture et la reconnaissance de mots. Cette analyse a montré que tous les participants ont réagi différemment selon les mots. En modélisant cette spécificité et en créant **un programme informatique**, les chercheurs ont réussi à identifier chaque personne **avec une précision de 94 %**. Au regard du panel et de la méthodologie relativement basique, il sera nécessaire de réaliser des tests plus complexes, preuve est faite que les ondes cérébrales peuvent être utilisées pour vérifier l'identité d'une personne. Donc qu'elles pourraient, en théorie, remplacer les mots de passe.

Cette technique aurait plusieurs avantages, explique Sarah Laszlo, professeur adjoint en psychologie et linguistique à l'Université de Binghamton et co-auteur de 'Brainprint' : *« la biométrie cérébrale est attrayante, car elle est annulable et ne peut pas être volée par des moyens malveillants contrairement aux empreintes digitales ou rétiniennes* ». En effet, « *si l'empreinte digitale est volée, la personne ne peut pas faire appel à un autre doigt pour la remplacer* », souligne la spécialiste en ajoutant que « *pour l'empreinte cérébrale en cas peu probable d'attaque, il est possible de faire un reset de cette empreinte* ».

Pour le professeur Zhanpeng Jin, expert en génie électrique et informatique, ainsi qu'en génie médical, « *nous voyons l'application de ce système de sécurité pour des endroits hautement sécurisés comme le Pentagone ou Air Force Labs, c'est-à-dire avec un nombre limité de personnes autorisées* ».

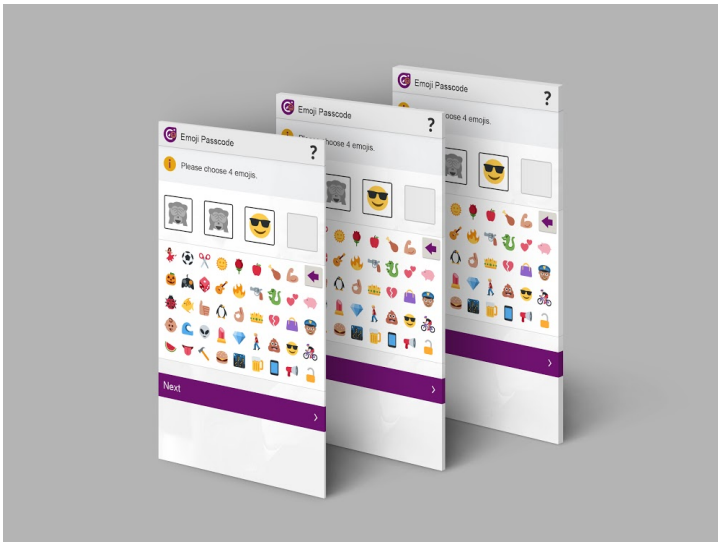
Battements du cœur, émoticônes, biométrie…

La recherche d'une alternative au mot de passe est récurrente, mais monte en puissance depuis quelques années. Pour plusieurs raisons. D'abord, les mots de passe sont devenus monnayables (des pirates russes ont volé 1,2 milliard de mot de passe ou plus récemment le piratage de Lastpass gestionnaire de mots de passe). La faiblesse de ces fameux sésames (lire l'article « 123456 reste toujours le mot de passe le plus utilisé ») est par ailleurs reconnue. Il ne se passe pas une semaine sans que ce système d'authentification ne soit cloué au pilori. Y compris les moyens pour retrouver les mots de passe. Google a ainsi considéré les questions de sécurité comme étant inefficaces. Le monde professionnel n'est pas exempt de reproches avec un comportement laxiste et quelques pratiques malhonnêtes.

D'autres techniques que les ondes cérébrales sont explorées comme moyen de substitution. Ainsi,

la banque britannique Halifax a testé un système de signature cardiaque pour connecter ses clients à ses services de paiements électroniques. De son côté, Windows 10 s'intéresse à la biométrie en embarquant FIDO 2.0 dans Windows 10. Cette norme permet l'authentification via la biométrie et un système multi-facteur. Est-ce que pour autant le mot de passe est mort ? Probablement pas. Des chercheurs se sont déclarés favorables à la réutilisation des mots de passe pour les comptes sans valeur. De même, les fournisseurs de service tentent d'aider les utilisateurs à gérer ou à générer des mots de passe, comme le fait Yahoo Mail ou Chrome de Google.

D'autres sont plus inventifs, comme la société britannique Intelligent Environments qui propose de se connecter à son compte bancaire en ligne **via des émoticônes**. Au lieu d'avoir un code PIN à 4 chiffres, l'utilisateur pourra choisir 4 images pour s'authentifier (cf photo ci-dessous).



A lire aussi :

Terminaux de paiement : un même mot de passe utilisé depuis 25 ans

Gestion des mots de passe : toujours du grand n'importe quoi

Google veut mettre fin aux mots de passe

Crédit Photo : Maksim Kabakou – Shutterstock