Mots de passe : les questions de sécurité inefficaces selon Google

Quel est le prénom de votre mère ? Ou quel est votre lieu de vacances préféré ? Ce genre de question pour réinitialiser un mot de passe perdu ne devrait plus être utilisé ou en tous cas pas comme seul moyen de protection. C'est ce que préconise une recherche menée par Google intitulée « *Secrets, Lies and Account Recovery* ». Elle a été menée sur un large panel des comptes Google (soit des millions de personnes) et montre que ces interrogations sont loin de garantir une sécurité optimale.

Ainsi, la banalité des questions et des réponses favorisent les attaques. Dans leur étude, les chercheurs ont réussi dans **20% des cas à répondre dès la première proposition** à la question « Quel est votre plat favori ? » pour les utilisateurs de langue anglaise. Ce taux monte à **39% au bout de 10 tentatives** pour les clients coréens se protégeant avec la question « *Quelle est votre ville de naissance ?* ». Pour les français, le taux de succès est relativement faible, car il faut une centaine d'essais sur la question « *Quel est le nom de votre meilleur ami* ?» pour atteindre 23,6%. Un petit tour sur les réseaux sociaux permet de glaner des informations précieuses pour répondre aux questions « secrètes ».

Des mensonges et des oublis

L'étude montre aussi le développement préjudiciable des fausses réponses. Pour être plus en sécurité, les utilisateurs choisissent de mentir à la question posée. Cela a une double conséquence. La première est l'oubli de la réponse et la seconde est le choix d'une réponse commune et donc facile à trouver. Ce dernier point est important, car l'oubli de la réponse est très rapide. Par exemple sur la question « *Plat favori ?* », l'étude montre que 74% des personnes se rappellent de leur réponse après 1 mois, 53% après 3 mois et 47% après un an. Le choix d'une question plus compliquée pourrait de la même façon se heurter au problème de mémorisation, ainsi qu'à des considérations techniques (car tous les fournisseurs ne proposent pas l'option de choisir sa question).

Les auteurs de l'étude soulignent que l'usage du **SMS et de l'email** revendique des taux de succès plus important pour la récupération des mots de passe. Même si chacun des outils à ses avantages et ses inconvénients. Le SMS est de plus en plus utilisé dans le cadre de la double authentification, mais peut s'avérer compliqué quand l'utilisateur est en déplacement dans des zones non ou peu couvertes. L'email secondaire est une autre voie intéressante, à condition que l'utilisateur regarde régulièrement son compte. In fine, le support des questions secrètes peut dans ce cas trouver sa place dans l'arsenal de protection. Pour les chercheurs de Google, la question reste ouverte.

A lire aussi :

Les salariés entre laxisme et cupidité sur leurs mots de passe
Carton rouge sur la gestion des mots de passe en France

Crédit Photo : Galam – Fotolia.com