

# FUTURA

## Les données génétiques de 6 millions d'individus piratés sur 23andMe

Podcast écrit et lu par Adèle Ndjaki

*[Générique d'intro, une musique énergique et vitaminée.]*

Des données génétiques privées qui s'échappent sur le web, c'est l'actu de la semaine dans Vitamine Tech !

*[Fin du générique.]*

La sécurité de nos données personnelles n'aura jamais été autant en danger. La société 23andMe, spécialisé dans les analyses génétiques, vient d'annoncer une nouvelle inquiétante : les comptes de plus de 6 millions de ses utilisateurs auraient été piratés. Lien de parenté et test ADN, les hackers ont réussi à mettre la main sur une vraie mine d'or, car les données très privées sont devenues particulièrement précieuses et susceptibles d'être exploitées et revendues sur le dark web.

*[Une musique électronique calme.]*

Panique à bord au sein de l'entreprise de tests génétiques 23andMe ! Si cette dernière a reconnu, il y a quasiment deux mois, le piratage des comptes de 14 000 de ses utilisateurs, la société américaine a révélé vendredi dernier que la situation serait bien plus grave qu'énoncé précédemment. En effet, d'après Andy Kill, le porte-parole de l'entreprise, les pirates auraient en réalité eu accès au compte de près de 7 millions de personnes, soit environ la moitié des utilisateurs revendiqués par l'entreprise. Car si dans un premier temps, 23andMe affirmait que les pirates avaient seulement pu avoir accès à certaines données personnelles de ses utilisateurs en fonction du type de compte et de la façon dont les internautes les avaient paramétrés, finalement, il s'avérerait qu'ils aient pu accéder à une plus grande quantité d'informations en utilisant une des fonctionnalités de leur service. Plus précisément, d'après la société américaine, ces voleurs 2.0 auraient d'abord réussi à dérober les données génétiques de 14 000 personnes en mettant en place un assaut par *credential stuffing*, c'est-à-dire en parvenant à se connecter à plusieurs comptes en utilisant des informations telles que des identifiants, ou des mots de passe réutilisés et obtenus sur d'autres sites piratés antérieurement. Puis dans un deuxième temps, grâce à l'accès à ces comptes, les assaillants ont pu utiliser la fonction « DNA Relatives », soit la fonction ADN partagé, qui permet aux individus de se connecter les uns aux autres en fonction des ancêtres qu'ils ont en commun, pour accéder à des informations supplémentaires provenant de millions d'autres profils. C'est ainsi que les pirates auraient progressivement pu capter

des données de 6,9 millions de personnes : en naviguant de compte en compte qui auraient un lien de parenté. L'ampleur des dégâts : les assaillants auraient en leur possession les noms d'utilisateurs de 5,5 millions de profils ayant la fonctionnalité ADN proche, leur pourcentage de patrimoine génétique commun, la localisation de certains individus ainsi que les lieux de naissance de leurs ancêtres et leurs photos de profil, entre autres. Concernant les 1,4 million d'internautes restant, les pirates auraient accès à leur arbre généalogique sans pour autant avoir cette fois-ci accès à des informations sur le pourcentage d'ADN partagé avec de potentiels parents sur le site, ni les segments d'ADN correspondants. Toujours selon l'entreprise 23andMe, il semblerait que les victimes proviennent de tout horizon économique, ou géographique, que ce soit de Chine, des États-Unis, d'Europe de l'Ouest ou encore du Moyen-Orient. Décidément, personne n'est à l'abri de se faire pirater de nos jours.

*[Virgule sonore, une cassette que l'on accélère puis rembobine.]*

*[Une musique de hip-hop expérimental calme.]*

Vous l'avez compris, la vie privée de près de 7 millions d'utilisateurs a pris un sacré coup. Cette violation aurait conduit à de multiples poursuites judiciaires envers la société américaine aux États-Unis et au Canada. En effet, plusieurs clients accuseraient l'entreprise de test génétique d'avoir manqué à ses obligations de sécuriser leurs informations personnellement identifiables et de ne pas avoir mis en place de mesures de sécurité adéquates. Une actualité qui vient démontrer l'importance qu'ont actuellement les données personnelles. Privacy Affairs, un site créé par des chercheurs en cybersécurité, ont d'ailleurs analysé les tarifs auxquels seraient vendues ces données si prisées sur le marché noir et affirmerait que les prix varieraient en fonction du document proposé mais également de son origine. Par exemple, un passeport français vaudrait en moyenne 2 740 €, plus qu'un passeport polonais qui coûterait 2 300 €, mais moins qu'un passeport maltais, d'on le prix s'élèverait à 3 650 €. Et attention, ces tarifs vaudraient autant pour des documents numérisés qu'en format physique. Le risque derrière tout ça : que l'on puisse facilement usurper votre identité. Conscient des enjeux qu'il y a derrière ce piratage de masse, 23andMe aurait donc conseillé à ses utilisateurs hackés de modifier leur mot de passe et aurait mis en place une authentification à deux facteurs pour tous ses clients. L'entreprise serait également en train d'informer tous les internautes concernés par l'attaque informatique. Si malheureusement le risque zéro n'existe pas en termes de hacking, des astuces existent pour compliquer la tâche de ces pirates informatiques comme mettre régulièrement à jour son appareil et l'éteindre une fois que ses tâches sont terminées, ou ne pas installer de logiciel dont l'origine ou la réputation sont douteuses. Mais l'une des clés pour mettre un frein conséquent à cette pratique illégale sera bien évidemment de créer le bon mot de passe. Pour ce faire, vous pouvez soit en inventer un de toute pièce comportant en tout 12 caractères, dont des chiffres, des lettres et des caractères spéciaux, ou encore vous pouvez en concevoir grâce à un générateur de mot de passe. Et pour encore plus de sécurité, n'hésitez pas à paramétrer sur votre PC la double authentification et tentez, si vous en avez la motivation, de fréquemment renouveler votre mot de passe.

*[Virgule sonore, un grésillement électronique.]*

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, encore une fois, pensez à vous abonner dès à présent et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous invite à découvrir notre dernier épisode de Bêtes de Science ou Agatha Liévin-Bazin vous emmène en Tanzanie, à la rencontre de la hyène tachetée. Pour le reste, je vous souhaite une excellente journée ou une très bonne soirée, et je vous dis à la semaine prochaine, dans Vitamine Tech.

*[Un glitch électronique ferme l'épisode.]*