La problématique des mots de passe

Ces derniers temps, on a assisté à une multiplication des attaques informatiques, parfois spectaculaires, qui ont notamment entraîné la compromission de bases de données entières de comptes et des mots de passe associés.

Dans ce contexte, il apparaît indispensable de fixer un niveau de sécurité élevé en la matière. Pourtant, de nombreux utilisateurs ne sont pas informés des pratiques élémentaires de sécurité et de gestion de leurs informations, alors que le nombre de comptes et la sensibilité de leurs informations ne cessent de croître et amènent une gestion toujours plus complexe de ces multiples comptes et de leurs mots de passes. Une gestion non organisée de ces mots de passe fait courir des risques aux utilisateurs sur ses données personnelles :

- l'utilisation du même mot de passe pour accéder à différents services peut compromettre les comptes sensibles, notamment les comptes bancaires et l'adresse de messagerie principale ;
- la tendance à partager ses mots de passe augmente les risques d'usurpation d'identité ;
- la tendance à créer des mots de passe en rapport avec soi (date de naissance, prénom des enfants, nom de son entreprise, etc.) les rend plus vulnérables, notamment dans un contexte où il est facile de récupérer des informations sur les personnes en ligne (ingénierie sociale) ;
- la difficulté à mémoriser un mot de passe trop long incite à définir des mots de passe trop simples, quelques caractères, souvent des mots usuels, ou à les écrire sur support papier.

La solidité des mots de passe

Par abus de langage, on parle souvent de « solidité » d'un mot de passe pour désigner sa capacité à résister à une attaque par une itération de tous les mots de passe possibles.

Cette « solidité » dépend de la longueur (**L**) du mot de passe et du nombre (**N**) de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire, hors des mots disponibles dans tous les dictionnaires de différentes langues. Elle se calcule aisément par la formule $L^{N)}$.

- $\mathbf{L^{10}}$ si le mot de passe ne contient que des chiffres
- $\mathbf{L^{26}}$ si le mot de passe ne contient que des lettres de l'alphabet totalement en minuscules ou en majuscules ;
- $\mathbf{L^{52}}$ si le mot de passe ne contient que des lettres de l'alphabet, avec un mélange de minuscules et de majuscules ;
- $\mathbf{L^{62}}$ si le mot de passe mélange les majuscules et les minuscules ainsi que les chiffres ;

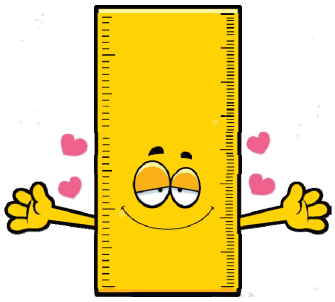
- **L^{90}** si le mot de passe mélange des majuscules, des minuscules, des chiffres ainsi que des caractères spéciaux,

Exemples du temps nécessaire à « casser » un mot de passe :

- 1234 = 4^{10} itérations - immédiat
- Snoopy = Existe dans les dictionnaires américains - 400 millisecondes
- mapomme = 7^{26} itérations 25 secondes
- TOaoqp2WCs (cheville phonétique de : Théo a occupé deux WCs) = 10^{62} 5 à 6 semaines
- Alf@-Romé0 (pour Alfa Romeo) = 10^{90} itérations > de mille ans

Une nuance cependant : les résultats donnés ne sont pas définitifs. Ils sont basés sur la puissance de calcul moyenne des PC actuels. Des ordinateurs avec des logiciels spécialement capables de réaliser de très nombreux calculs en très peu de temps peuvent cracker les mêmes mots de passe beaucoup plus rapidement. De plus, ces capacités de calcul seront forcément accrues dans les prochaines années !

Les règles d'or pour protéger votre mot de passe



- Votre mot de passe doit être robuste : long et complexe, avec des majuscules, minuscules, chiffres et si possible caractères spéciaux, mais attention aux caractères spéciaux lorsque vous utilisez des langues différentes avec votre clavier.
- Activez la double authentification si elle est disponible, En général, un code à usage unique doit être renseigné en plus du mot de passe habituel de l'utilisateur.
- Il n'est connu que de vous et vous ne devez jamais le communiquer à qui que ce soit, sauf peut-être à votre conjoint-e.
- Ne l'écrivez pas sur un papier, sous le tapis de souris ou sur votre téléphone mobile.
- Ne l'enregistrez pas dans votre navigateur internet. Les navigateurs internet vous proposent de sauvegarder le mot de passe que vous avez saisi lors d'une connexion à un site. Si vous acceptez, un autre utilisateur de votre ordinateur qui accède au même site avec le même navigateur peut obtenir votre mot de passe et se connecter en utilisant votre identifiant.
- Ne l'enregistrez pas dans votre messagerie internet, sur un réseau social ou dans une application internet. Le niveau de sécurité de ce type de services étant variable, il est risqué de les utiliser pour stocker des informations confidentielles ou secrètes. Par exemple, il n'est pas avisé de s'envoyer un courriel contenant un mot de passe pour s'en souvenir ultérieurement, un tiers prestataire pourrait l'obtenir et l'utiliser pour accéder indûment à l'information protégée par ce mot de passe.
- Utilisez des mots de passe différents pour chaque site ou application pour éviter qu'un mot de passe compromis donne accès à plusieurs sites.
- Changez-le régulièrement et dès que vous avez un doute sur sa sûreté.
- Sachez que les banques, organisations administratives, cartes de crédits, helpdesks, etc. ne vous demanderons jamais vos mots de passe par email ou par appels téléphoniques de leur part.

Le séquestre des mots de passe

Nos pauvres petits neurones conservent tant bien que mal toujours plus de sésames, et nous ne sommes pas éternels et il serait dommage qu'avec nous disparaissent les accès à un héritage numérique, par exemple les mots de passe de nos accès bancaires, nos courriels, notre agenda, notre liste de contacts, nos photos, etc., nos héritiers peuvent en avoir besoin.

La méthode la plus simple pour organiser et conserver ses mots de passe est de les consigner dans une feuille Excel™ protégée elle-même par un mot de passe solide. Les informations à enregistrer sont :

- La date de création du mot de passe (ou de son changement)
- Le nom de l'organisation
- L'identifiant utilisé pour la connexion au compte ***Attention*** *: souvent votre adresse email est demandée comme identifiant pour la création d'un compte client, dans ce cas utilisez un autre mot de passe que celui de votre email.*
- Le mot de passe
- L'URL (lien https:// pour se connecter)
- Remarques

Quelques logiciels gestionnaires de mots de passe et centrés sur la sécurité.

Les données sont cryptées pour que vous soyez le seul à accéder à vos informations. En plus de la fonction de coffre-fort, ces logiciels génèrent des mots de passe solides et permettent d'établir la connexion.

Attention : téléchargez le logiciel à partir du site auteur du logiciel, pas depuis d'autres sources dont on ne sait pas si le logiciel a été modifié avec des vulnérabilités (portes cachées) de sécurité.

- **Keypass** https://keepass.info/ logiciel open source gratuit, certifié par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) et recommandé par l'Etat français.
- **Lockpass** https://www.lockself.com/solutions/LockPass-gestionnaire-mot-passe logiciel payant certifié par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information),
- **1Password** https://1password.com/fr/ logiciel payant plutôt pour PME et grandes entreprises.
- Et bien d'autres encore

Note : les mots de passe peuvent être remplacés par la biométrie, empreinte digitale ou reconnaissance faciale, mais c'est beaucoup plus complexe à gérer pour un utilisateur lambda.

Claude Maury – *certifié auditeur ISO/IEC 27001 durant ma carrière professionnelle*

Sources :

ISO/IEC 27001 Exigences relatives aux systèmes de management de la sécurité des informations

ANSSI - Agence Nationale de Sécurité des Systèmes d'Information (France)