Vos mots de passe sont-ils vraiment sécurisés ❓

Plan 🗒 :

• Comment crée un mot de passe sécurisé ?

• Complexité d'un mot de passe avec les combinatoires

Introduction :

Que ce soient les Messageries, réseaux sociaux, banques, administrations ou commerces en ligne. La sécurité de tous ces services que nous utilisons tous les jours repose essentiellement sur les mots de passes. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de Cybercriminalité, ransomware, usurpation d'identité, et de diffusion de données privées. Selon cyclonis, Aujourd'hui 83% des utilisateurs utilisent le même mot de passe sur plusieurs sites C'est pourquoi il est nécessaire d'avoir des mots de passes forts : complexes.

Partie NSI

Je vais vous montrer comment rendre nos mots de passe plus sûr et plus sécurisé.

La première étape est de ne pas utiliser un mot de passe similaires pour différents sites ou application. Ce n’est pas facile mais énormément d’outils aujourd’hui nous permet de les retenir pour nous, ce sont des gestionnaires de mots de passes

Selon la CNIL et l'ANSSI (Agence nationale de la sécurité des systèmes d'information), Un bon mot de passe doit contenir au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.

De plus, il ne doit pas contenir d'informations susceptibles d'être devinées (nom, nom d'animal, date de naissance...).

Aussi, il est conseillé d'utiliser les modules de double authentification, qui demandent une confirmation supplémentaire (par sms, courriel électronique ou code temporaire) afin de permettre une connexion.

Il est aussi précisé qu'il faudrait renouveler ses mots de passes tous les 90 jours, les gestionnaires de mots de passes savent aussi effectuer ces actions automatiquement.

On pourrait se dire qu’un pirate ne peut que trouver un mot de passe grâce à notre vie, notre date de naissance, le nom de notre chien mais non.

Aujourd’hui il existe des algorithmes capables de trouver nos mots de passes rapidement par exemple avec un algo de brute force :

• Il essaye toutes les solutions possibles

• Plus le mot de passe est court et simple, plus rapidement il peut être craqué avec la méthode de force brute.

• C’est pour cela qu'on conseille des mots de passes avec différents caractères

Mais en combien de temps un algo de ce type trouve nos mots de passes en moyenne ?

• Code de téléphone : Instantanément

• Mdp 7 caractères (maj + min) Instantanément

• Mdp 10 caractère (maj + min + chiffre) 3 jours

• Mdp 18 caractères (8 lettres (52), 6 chiffres (10), 4 car. spé. (10)) 438 billions d’années

Solution : blocage d’IP automatique (attention parade avec VPN)

Pour le public : utiliser des modules de double authentification

Partie Mathématique Dénombrement

Nous pouvons Démontrer avec le dénombrement que plus il y’a de caractères sur un mot de passe plus il est compliqué de le trouvé et donc juste en ajoutant des caractères spéciaux et quelques chiffres on peut largement améliorer la complexité de vos mots de passes.

Nous allons alors comparer le nombre de combinaisons possibles pour différents types de mot de passes :

• Code de téléphone à 4 chiffres 10^4 = 10 000

• Un digicode d’appartement de 4 chiffre suivi d’une lettre (A ou B)  :

• Mdp 18 caractères (lettres (52), chiffres (10), 4 car. spé. (10)) =

Dans chaque cas de figure, il y a remise, un caractère peut évidemment être utilisé plusieurs fois par le mot de passe.

K-uplet car rep + remise

On constate alors que plus le nombre de combinaisons possibles est élevé, plus la probabilité qu'un robot ou qu'une personne mal intentionnée trouve la bonne combinaison est faible.

Conclusion

Donc si vous n’utilisez pas de système de double notification et que vous utilisez un même mot de passe sur différents sites Web ou applications et que votre mot de passe ne comporte pas au moins 12 caractères et quatre types de caractères différents votre mot de passe n’est pas sécurisé