

Les mots de passe les plus populaires en 2022

S curit 

Post  par : JerryG

Publi e le : 13/2/2023 13:00:00

Tout d'abord, une mauvaise nouvelle pour les fain ants : les mots de passe doivent r pondre   un niveau minimum de s curit , et donc de complexit . Trop souvent, ce n' tait pas le cas l'ann e derni re, comme l'a montr  par exemple l'Institut Hasso-Plattner.

Cet institut informatique  value chaque ann e les mots de passe les plus utilis s en Allemagne et, comme les ann es pr c dentes, il est arriv    une conclusion qui donne   r fl chir pour 2023.

La premi re place est occup e par la combinaison simple de chiffres "123456", qui devance la deuxi me version la plus fr quente, l' g rement plus avanc e, "123456789". Les dix meilleurs mots de passe allemands de 2022 montrent sans aucun doute une marge d'am lioration consid rable.

Mais il y a aussi de bonnes nouvelles pour ceux qui sont agac s par ce qui est souvent d fini comme une norme de s curit  : les mots de passe s curis s n'ont pas besoin de 20 caract res et n'ont pas besoin d' tre modifi s mensuellement.

  De nombreuses r gles de mot de passe bien connues sont maintenant consid r es comme obsol tes. C'est principalement parce qu'ils sont difficilement r alisables dans les applications quotidiennes.

Important : utiliser des mots de passe diff rents

Aujourd'hui, l' ternetaute lambda doit m moriser un nombre consid rable de mots de passe. Nous nous connectons quotidiennement pour acc der   nos comptes bancaires, aux sites de e-commerces, aux r seaux sociaux et aux services de streaming.

Notre vie devient de plus en plus num rique, et par cons quent, les mots de passe envahissent nos vies.

Il est irr aliste de s'attendre   ce que quelqu'un m morise des mots de passe multiples, divers et longs, qui doivent  tre chang s r guli rement, sans quelque chose pour nous aider   les retenir.

Th oriquement, la m morisation serait la m thode la plus s re, mais elle  choue dans la pratique. M me l'Office f d ral allemand de la s curit  de l'information (BSI) l' a reconnu et a supprim  plusieurs conseils traditionnels et bien intentionn s dans ses derni res recommandations pour la communication concernant la s curit  des mots de passe.

Le plus important de nos jours est d'utiliser diff rents mots de passe pour diff rents comptes. La raison est facile   comprendre: c'est d j   assez grave si un mot de passe tombe entre de mauvaises mains.

Et les dommages peuvent  tre rapidement minimis s si, par exemple, les intrus n'ont qu'un bref acc s   un service de streaming.

En revanche, si la combinaison d'une adresse électronique et d'un mot de passe ouvre tout le coffre-fort numérique d'une personne, les dommages peuvent devenir considérables.

En isolant les données d'accès individuelles, un changement de mot de passe n'est vraiment nécessaire que si le service en question a subi une violation de données.

A leur tour, et en fonction de l'importance d'un compte, les mots de passe individuels peuvent être un peu moins complexes, mais certainement pas aussi simples que « 123456789 ».

La question qui se pose naturellement est de savoir comment se souvenir de tant de mots de passe différents.

.../..