PARIS : Voici les mots de passe les plus populaires, ceux à définitivement oublier !

Découvrez les mots de passe les plus utilisés – et pourquoi il faut absolument les éviter pour parer aux cyberattaques et assurez votre sécurité en ligne !

Les mots de passe constituent la première étape essentielle pour votre défense en ligne, pour protéger vos données et votre vie privée. Mais l'efficacité de votre défense en ligne ne vaut rien si la sécurité du mot de passe en question est insuffisante.

Pour comprendre si un mot de passe est sécuritaire, il faut se pencher sur les moyens que déploient les cybercriminels pour accéder aux données qu'il protège. Ils ont plusieurs outils à leur disposition pour cela. Parmi ceux-ci, les attaques par dictionnaire : il s'agit de tenter de déchiffrer les mots de passe en utilisant un à un ceux indiqués dans une base de données regroupant des mots de passe courants ou facile à déterminer. Contrairement à une attaque par force brute, qui teste l'ensemble des combinaisons possibles, on cible ici les mots de passe les plus probables.
On comprend donc que l'utilisation de mots de passe courants, qui ont déjà été piratés, ou faciles à deviner, sont particulièrement fragiles à ce type d'attaques et doivent être évités.
Chaque année, l'entreprise SplashData, spécialisée dans la sécurité des mots de passe, publie une liste annuelle des mots de passe les plus couramment utilisés sur le Web, basé sur son examen de plus de cinq millions de mots de passe divulgués par des cybercriminels. Le palmarès 2019 devrait être publié sous peu. On peut néanmoins se baser sur les palmarès des dernières années pour se faire une idée du type de mots de passe qu'on y retrouve.

Voici le Top 10 des deux dernières années :

Position 2018 2017
1 123456 123456
2 password Password
3 123456789 12345678
4 12345678 Qwerty
5 12345 12345
6 111111 123456789
7 1234567 Letmein
8 sunshine 1234567
9 qwerty Football
10 iloveyou Iloveyou

On peut facilement constater ici que les suites numériques

sont à proscrire, tout comme les mots et expressions trop simples (» password » et » qwerty « , par exemple). Notez qu'on y trouve également des mots liés au sport ou à l'actualité dans le palmarès. Ainsi, » donald » figurait au 23e rang du palmarès 2018. Les suites de lettres ou de chiffres simples, telles » abc123 » ou » qwerty123 » se démarquent également, ainsi que les suites de caractères spéciaux telles que » !@#$%^&* » (obtenu en gardant la touche Majuscule enfoncée et en entrant » 12345678 » sur un clavier anglais).

Évidemment, il ne suffit pas d'éviter les 50 ou 100 pires mots de passe pour être protégés.

Cependant, ces listes nous permettent de dégager des principes sur l'élaboration de mots de passe plus sécuritaires :

Éviter de choisir des mots que ce soit des noms communs, noms propres, verbes… et quelle que soit votre langue. Évidemment, les internautes anglo-saxons sont plus nombreux, mais les cybercriminels et leurs outils ne connaissent pas de barrière linguistique quand vient le temps de déchiffrer les mots de passe

Éviter les séries de caractères facilement déchiffrables. Qu'on parle de lettres, chiffres, caractères, ou d'une combinaison de ceux-ci, les suites simples à deviner sont une cible trop facile pour les criminels.

Vérifiez si vos mots de passe ont déjà été identifiés dans une brèche de données. Si c'est le cas, même si c'est parce qu'un autre utilisateur a été piraté, sur une autre plateforme, un mot de passe déjà disponible publiquement est peu sécuritaire, et ne devrait jamais plus être envisagé.
Peut-être vous dites-vous que votre profil ne contient pas d'information compromettante et qu'un piratage ne serait pas si dramatique ?
Mais est-ce réellement le cas ? Votre compte de streaming en

ligne contient certaines informations bancaires, vos programmes de récompense permettent de déduire vos habitudes d’achats et votre adresse, vos profils de médias sociaux incluent probablement des photos, des dates marquantes, votre adresse de courrier électronique, etc. En utilisant un mot de passe sécuritaire et distinct pour chacun de vos accès numériques, vous amélioreriez la protection de toutes vos informations personnelles.

Benoit Grunemwald
Expert en Cyber sécurité,
ESET France