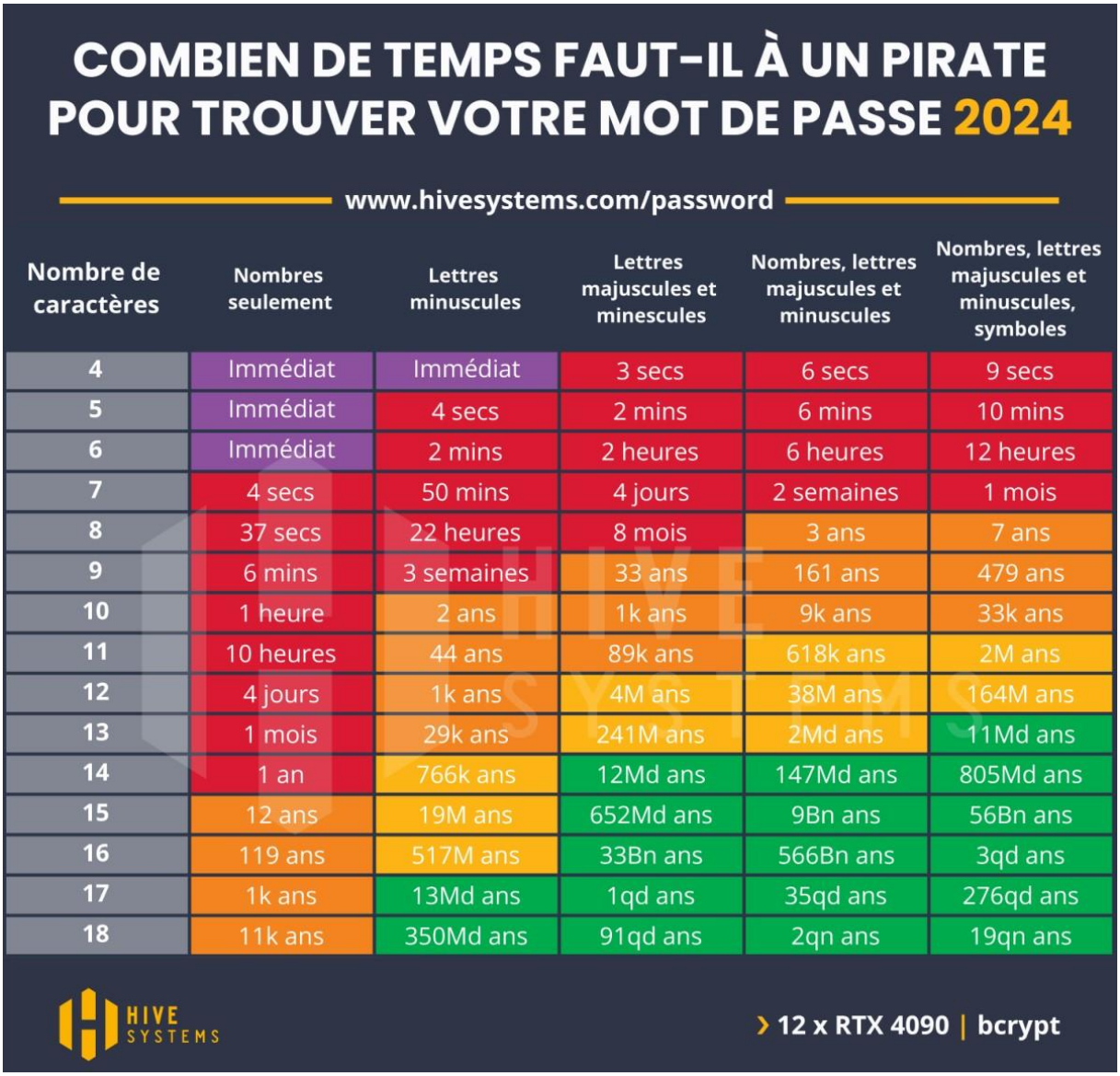
Asprom **le futur de l'innovation**

votre mot de passe en 2024 ?

Blog du Moderateur - BDM

Certains mots de passe peuvent être piratés en quelques secondes selon la dernière étude de Hive Systems.

Hive Systems, entreprise spécialisée dans les systèmes de sécurité informatique, vient de publier son tableau annuel qui met en lumière le temps nécessaire pour forcer un mot de passe en fonction de son nombre de caractères et de ses spécificités (minuscules, majuscules, chiffres, caractères spéciaux).



Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

Alors, est-il temps de changer vos mots de passe ? © Hive Systems

Les mots de passe de moins de 8 caractères ne sont pas efficaces

Le tableau vient confirmer ce qui est déjà constaté depuis plusieurs années dans le domaine de la cybersécurité : un mot de passe n'est pas sécurisé s'il est trop court et trop simple dans son contenu. À titre d'exemple, un mot de passe de 5 caractères qui ne contient que des lettres minuscules peut se faire hacker en seulement 2 minutes !

Pour un mot de passe réellement sécurisé, il n'y a qu'une seule solution : ajouter de la complexité. En alliant les bons éléments à son mot de passe, le temps de piratage nécessaire augmente fortement. Ainsi, selon les données du tableau, il faudra environ 479 ans pour déchiffrer un mot de passe de 9 caractères, contenant des lettres minuscules, des lettres majuscules et des caractères spéciaux.

Notre tableau des mots de passe se concentre sur l'idée selon laquelle le pirate informatique évolue dans une situation de « boîte noire » et doit repartir de zéro pour déchiffrer votre hachage afin d'afficher le « pire des cas » ou le « temps maximum requis », précise Hive Systems.

À noter que la méthodologie diffère de l'an dernier comme le souligne le rapport : « Dans les années précédentes, le hachage de mot de passe que nous utilisions était MD5, nous ne voyons pas autant de MD5 dans les violations de sécurité, ce qui signifie probablement que les sites web et les entreprises l'utilisent moins (ce qui est une bonne chose !). En conséquence, nous avons mis à jour le tableau des mots de passe de cette année pour utiliser bcrypt, qui est un hachage de mot de passe plus robuste, ce qui a « repoussé le violet » vers le haut – mais cela ne durera probablement pas, puisque la puissance de calcul augmentera dans les années à venir. »

Comment renforcer la sécurité de vos comptes ?
La méthode la plus simple est de s'appuyer sur un gestionnaire de mots de passe car pour chaque création de compte, il vous sera proposé un mot de passe robuste et unique, généré automatiquement. Pour une protection renforcée, vous pouvez également vous appuyer sur des applications de double authentification. Il est important de ne pas négliger la sécurité de ses comptes dans une période où les cyberattaques se multiplient.

« Et si on arrêtait d'utiliser des mots de passe ? » Une autre solution est en train d'émerger et peut s'avérer intéressante pour sécuriser ses comptes : **les passkeys**. Cette technologie d'identification vous permet de vous connecter sans mot de passe. Vous pouvez d'ores et déjà tester ces passkeys sur Google, Microsoft et WhatsApp.

Passkeys : tout savoir sur ce système d'authentification qui veut remplacer les mots de passe

En mai dernier, Google annonçait la prise en charge d'un nouveau système d'identification : les passkeys, ou clés d'accès. Quelques mois plus tard, il faisait des passkeys son système d'identification par défaut. Presque inconnues il y a un an, les clés d'accès semblent se développer à une vitesse telle qu'elles pourraient, dans un futur proche, remplacer les mots de passe. En effet, de

nombreux autres acteurs ont suivi cette tendance, comme Apple, Microsoft, WhatsApp, et même TikTok. Alors, en quoi consistent les passkeys, et que changeront-elles concrètement ? On vous dit tout !

Qu'est-ce qu'une passkey ?

Les passkeys représentent une technologie d'authentification qui utilise des données chiffrées. Ils sont développés par l'Alliance FIDO, une association qui vise à offrir des alternatives sécurisées aux mots de passe.
L'authentification s'opère en deux étapes :

La reconnaissance de l'appareil : lorsque vous vous inscrivez à un service ou une application, deux clés sont générées, une publique et une privée, qui fonctionnent en tandem. La clé privée, liée à l'appareil, interagit avec la clé publique, intégrée au service ou à l'application. Au moment de la connexion, la clé publique reconnaît la clé privée.
La reconnaissance de l'utilisateur : pour s'assurer que le smartphone est bien utilisé par son propriétaire, une seconde couche d'authentification est opérée. L'utilisateur peut alors sélectionner la méthode qui lui convient : déverrouillage biométrique, empreinte digitale, code PIN, schéma, etc.

Les passkeys : plus sécurisées que les mots de passe

Régulièrement, les mots de passe sont pointés du doigt pour leurs failles en matière de sécurité. Selon une étude menée par Specops Software, un mot de passe de 10 caractères, composé de majuscules et de minuscules, peut être déchiffré en seulement 2 jours par un hacker. Les spécialistes de la cybersécurité s'accordent également à dire que, pour une connexion sécurisée, les utilisateurs devraient utiliser un mot de passe différent pour chaque compte. Inutile de préciser que la majorité des internautes sont loin de suivre ces recommandations.

Les passkeys apparaissent alors comme une alternative crédible. Les informations d'identification n'étant pas stockées sur un serveur central, les pirates ne peuvent envisager d'attaque à grande échelle. Les passkeys offrent également une protection presque infaillible contre le phishing. Pour les utilisateurs, ce système a pour avantage d'éviter de retenir une multitude d'identifiants complexes.

Pour autant, les mots de passe ne devraient pas disparaître de sitôt. Fermement ancrés dans les habitudes des utilisateurs, leur obsolescence devrait être progressive, et rien n'assure que les passkeys parviendront à faire l'unanimité.

Apple, Google, Microsoft : les passkeys sont-elles interopérables ?

Les passkeys sont encore en construction, et la parfaite interopérabilité entre les différents écosystèmes sera une condition nécessaire à leur adoption par le plus grand nombre. En d'autres termes, il est essentiel que les utilisateurs puissent utiliser un seul et même système pour se connecter aux produits Windows, Android ou iOS.

En effet, les clés privées sont stockées localement sur un appareil (smartphone, PC ou tablette) et, à ce jour, chaque écosystème permet la synchronisation des clés d'accès sur son cloud (Drive pour Google, iCloud pour Apple ou OneDrive pour Microsoft). Cependant, la compatibilité entre les systèmes d'exploitation n'est pas optimale. Le transfert des passkeys est possible, notamment via un système de QR code, mais la synchronisation pose encore problème. Cette situation complique l'utilisation de produits issus d'écosystèmes différents – par exemple un smartphone Android avec un Mac – ou lors d'un changement d'appareil d'un écosystème à un autre.

Mais cette problématique pourrait être résolue prochainement. En effet, les géants de la tech, tels que Google, Apple et Microsoft sont favorables à la transition vers les passkeys, et ont intérêt à en faciliter l'accès. Membres du conseil d'administration de l'Alliance FIDO, aux côtés d'autres grands noms comme Samsung, Amazon ou Meta, ils travaillent activement à l'amélioration des normes d'interopérabilité, comme le confiait le directeur exécutif de l'association, Andrew Shikiar, au journal Le Monde il y a un an.
Il existe le site Passkeys.directory qui recense les principaux sites et services qui acceptent les passkeys.

Quels sont les atouts du passkey par rapport au mot de passe ?

Les passkeys présentent plusieurs avantages par rapport aux mots de passe :

- **Il n'est pas nécessaire de les mémoriser** ;
  Ces codes d'identification (pour les clés privées) sont stockés exclusivement sur les appareils appartenant à un même individu — en gros, ceux qui sont connectés au même compte, par exemple, de Google, de Microsoft ou d'Apple. Ces codes peuvent être synchronisés d'un appareil à l'autre. Les terminaux, en somme, deviennent des sortes de gestionnaires de mots de passe (de passkeys, précisément). Ce sont eux qui mémorisent tout.

- **Les passkeys sont robustes par défaut** ;
  Les codes d'identification ne sont pas du genre à rassembler à toto123 ou à des horreurs similaires. Chaque clé est suffisamment longue et solide (pour avoir une petite idée, elles ressemblent à ce genre de charabia) pour que

l'on ne puisse pas la deviner. Elles ne sont pas non plus réutilisées ou faibles. Ce sont des codes uniques. Exactement ce qu'il faudrait faire avec ses mots de passe, en fin de compte

- **Les fuites de données ne sont pas un problème (pour les passkeys) ;**
  Les serveurs n'hébergent à aucun moment les clés privées liées aux passkeys. Ils n'ont accès qu'aux clés publiques. Il est impossible d'employer l'une pour retrouver l'autre. Dès lors, ces données sont moins intéressantes pour les pirates. Pour avoir les clés privées, il faudrait cibler l'appareil de chaque internaute. La tâche est bien trop dure pour une action à grande échelle. Ce qui peut toujours fuiter, par contre, ce sont d'autres données personnelles.
- **Le phishing est contré ;**
  Il n'y a plus de mots de passe avec les passkeys, donc il n'y a rien à hameçonner ici. Les codes d'accès sont liés intrinsèquement à l'application ou au site pour lequel ils ont été créés. Même si une application frauduleuse ou un site piégé imite à la perfection l'app ou le service légitime, le système verra bien qu'il y a un souci avec le domaine. Il notera l'absence de clé publique (qui n'est pas en possession du site truqué, mais bien du site légitime).

Et les mots de passe alors ? Quel sera leur avenir face aux clés d'accès ?

Si les passkeys sont peut-être l'avenir de la sécurité informatique, c'est un futur qui n'adviendra pas à brève échéance. On peut le supposer en observant la vitesse avec laquelle se propage la double authentification chez le grand public : tout le monde ne s'en sert pas, alors que cela fait des années que des solutions sont à disposition de tous sur nombre de sites et de services.

Les deux solutions devraient d'ailleurs cohabiter pendant un long moment. Les gestionnaires de mots de passe n'ont donc pas d'inquiétude à se faire dans l'immédiat, même si les principaux ont commencé l'an dernier à s'adapter pour être aussi des gestionnaires de passkeys. C'est le cas de Dashlane, 1Password, LastPass et Bitwarden, notamment.

La longue traîne de l'adoption des passkeys promet d'être diablement étendue et, ce faisant, les mots de passe ne sont pas près de passer l'arme à gauche. Une fois la vague des early adopters passée, il faudra engager la bascule du grand public, des entreprises, des institutions publiques et de tout ce qui utilise un mot de passe. Rien ne dit que tout le monde sautera le pas.