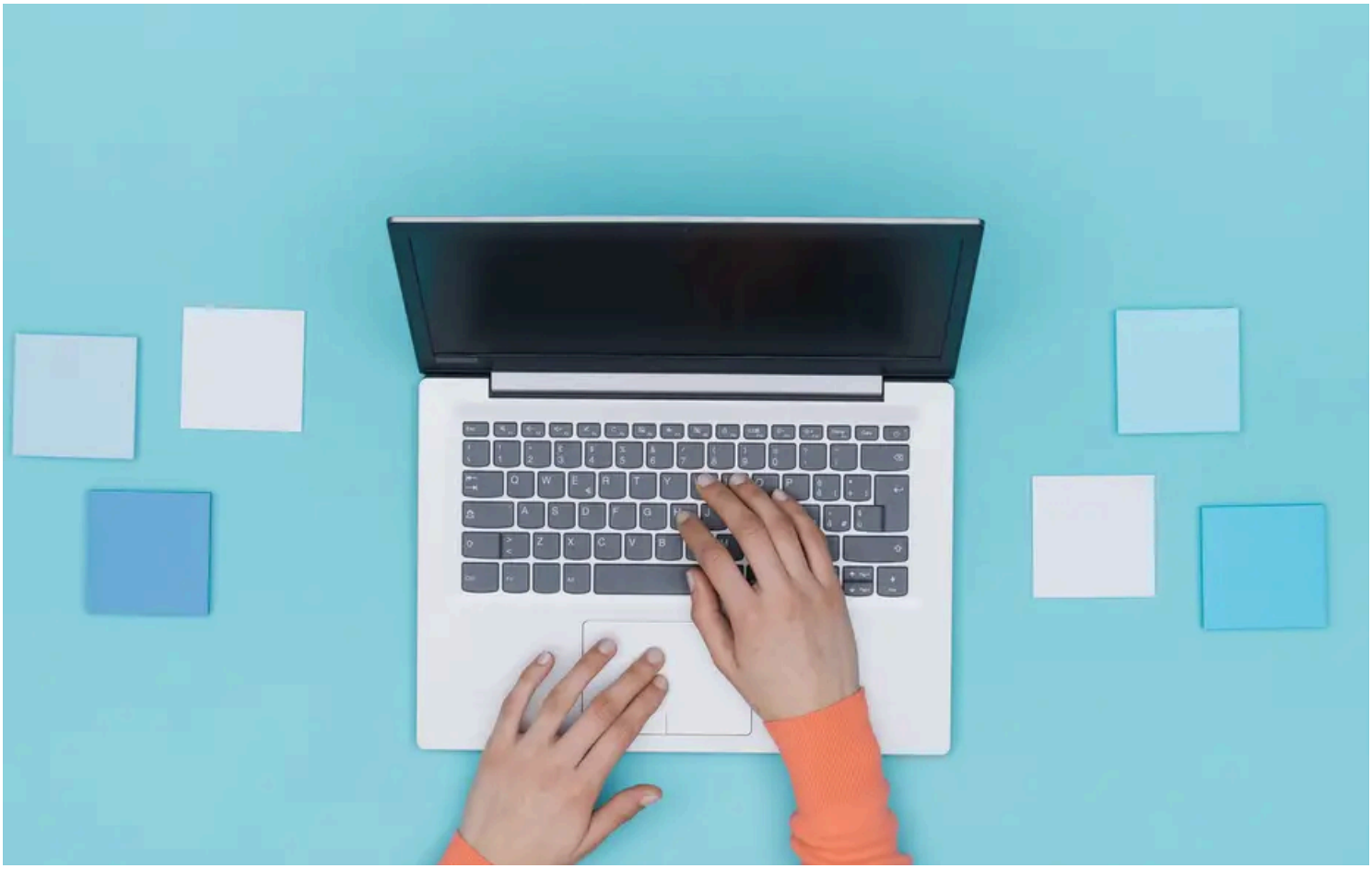
www.popsci.com /diy/how-to-check-your-passwords/

Comment vérifier la force de votre mot de passe et ce qu'il faut faire pour y remédier

Ne vous laissez pas vulnérable.

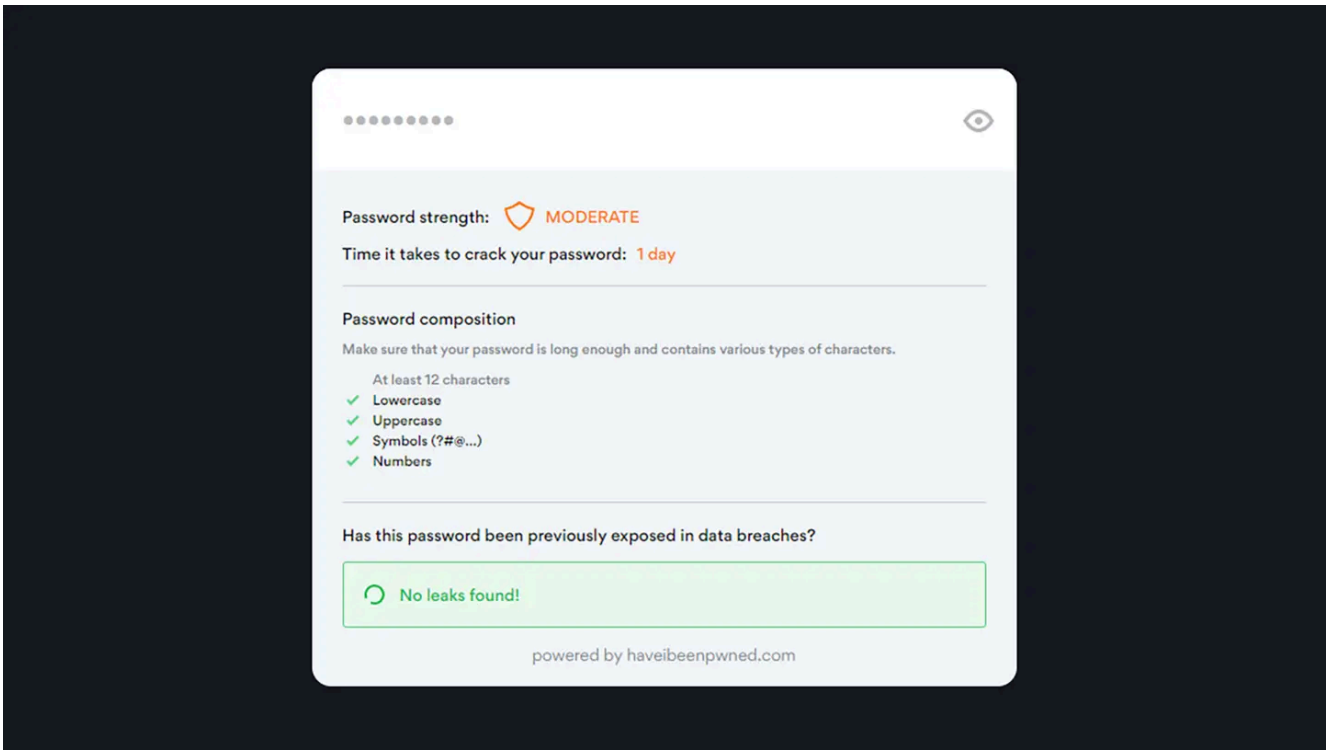
David Nield :



Bien que la connexion à l'aide d'une empreinte digitale ou d'un scan du visage soit de plus en plus courante, les mots de passe restent essentiels pour de nombreuses applications et services que nous utilisons tous les jours.
Et des achats aux opérations bancaires, des médias sociaux à la messagerie, des podcasts au stockage dans le cloud, il y a beaucoup de comptes et de mots de passe à suivre.

Vos mots de passe sont tout ce qui se dresse entre les mauvais acteurs et vos précieuses données, et bien sûr, vous ne voulez pas que tout le monde se promène dans vos espaces en ligne.
En gardant cela à l'esprit, il est crucial que vos mots de passe soient à l'épreuve du piratage, et nous avons rassemblé quelques moyens de mettre cela à l'épreuve.

Qu'est-ce qu'un mot de passe fort ?



Il y a des règles à suivre si vous voulez que vos mots de passe soient forts. Capture d'écran : NordPass

Le vieil adage sur les mots de passe est qu'ils devraient être impossibles à deviner et très difficiles à oublier - vous avez sans doute vu ces scènes dans les films où le mot de passe de quelqu'un est deviné, avec des dates significatives, des noms, des phrases et des animaux de compagnie généralement tous essayés.
Bien sûr, il n'est pas toujours facile d'essayer de trouver l'équilibre entre quelque chose d'indevable et d'inoubliable.

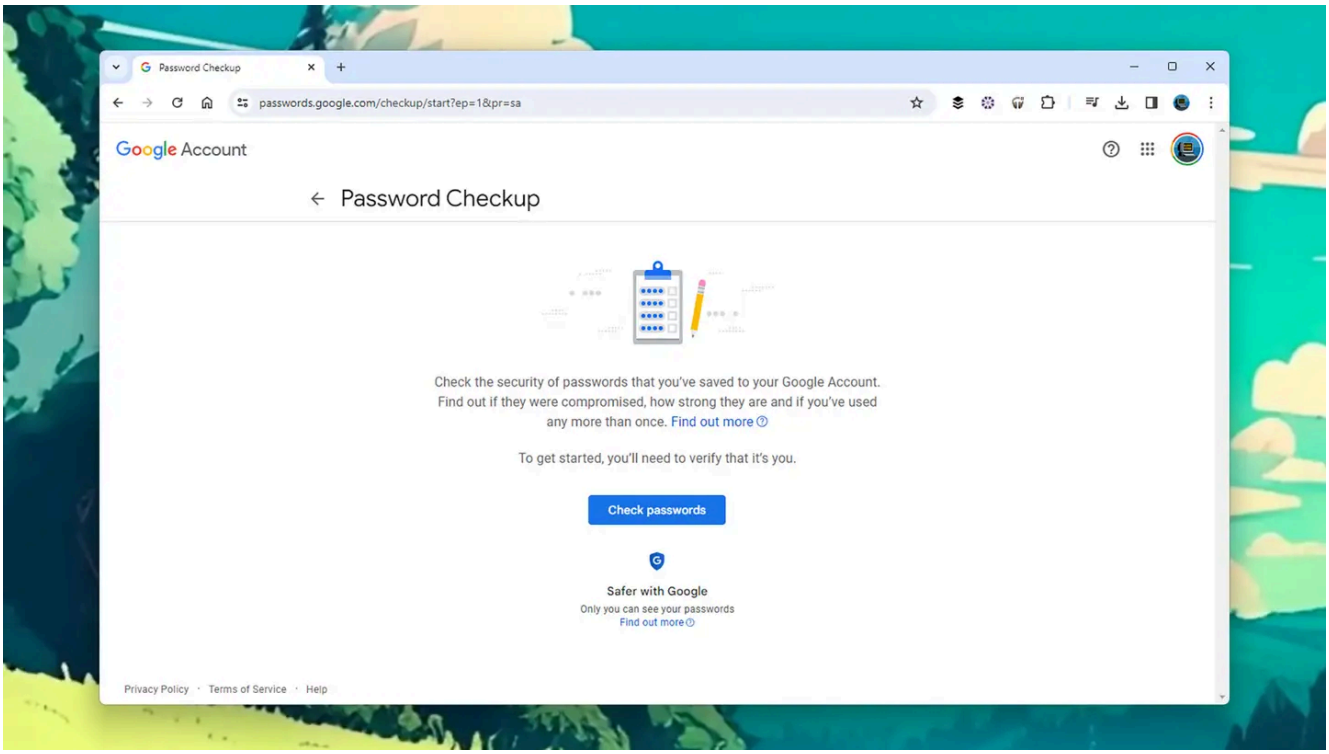
Les mots de passe plus longs sont préférables, tout comme les mots de passe qui incluent des caractères spéciaux (comme des points d'interrogation) et des chiffres, ce qui rend les attaques par force brute, où de nombreuses combinaisons différentes sont essayées en succession rapide, beaucoup moins susceptibles de réussir.
Évitez les mots et les phrases bien connus, ainsi que les noms (de personnes, de marques ou d'entreprises).

La réutilisation des mots de passe rend la vie numérique plus pratique, mais c'est quelque chose que vous ne devriez jamais faire : cela facilite la vie des pirates, et si l'un de ces comptes est compromis, tous les autres avec le même mot de passe peuvent rapidement suivre.
Cela peut prendre plus de temps, mais vous devez toujours créer des mots de passe individuels et forts pour tous vos comptes.

Alors, comment garder une trace de tous ces mots de passe complexes et uniques ?
Il est recommandé d'utiliser un gestionnaire de mots de passe ou d'utiliser les outils intégrés à votre navigateur Web.
Il est également possible d'écrire des mots de passe, à condition que ces notes soient cachées dans un endroit sûr et sécurisé, et non (par exemple) collées sur des notes autocollantes juste à côté de votre ordinateur portable.

Si vous avez besoin de les écrire, pensez peut-être à écrire des indices plutôt que les mots de passe eux-mêmes.

Comment vérifier vos mots de passe



Le gestionnaire de mots de passe de Google peut vérifier la force du mot de passe.
Capture d'écran : Google

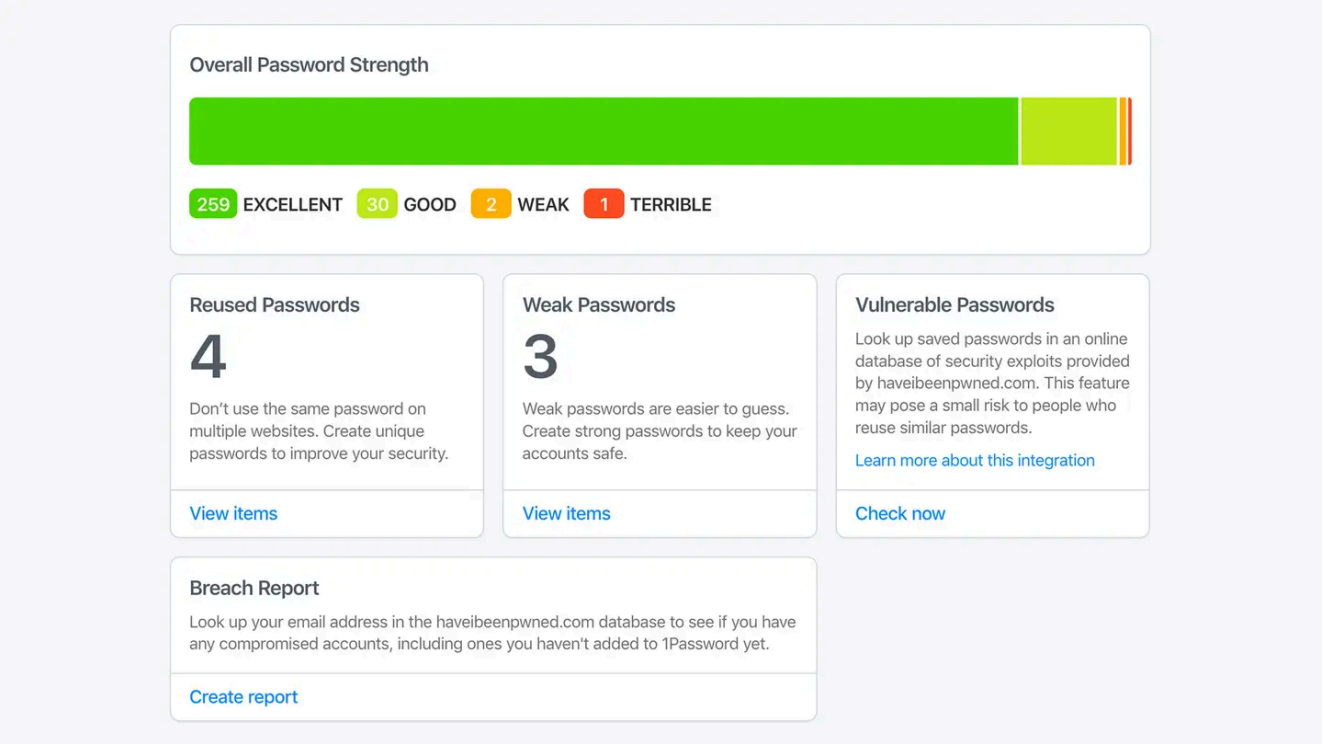
De nombreuses applications et sites Web sont disponibles pour vérifier la force de vos mots de passe pour vous : vous pouvez même voir un indicateur qui passe du rouge à l'orange puis au vert lorsque vous tapez un mot de passe pour un nouveau compte. Lorsque vous vous inscrivez à quelque chose de nouveau, vous pouvez recevoir des directives que vous devez suivre, comme l'inclusion d'un personnage spécial, par exemple.

Nous aimons le vérificateur que le gestionnaire de mots de passe NordPass a mis en ligne.
Tapez l'un de vos mots de passe (le mot de passe ne sera pas enregistré) et vous serez informé de sa force ou de sa faiblesse, ainsi que des raisons.
Vous verrez également une estimation du temps nécessaire pour déchiffrer le mot de passe, ainsi qu'une alerte si votre mot de passe est apparu dans une violation de données.
Des outils similaires sont disponibles auprès de Bitwarden et Security.org, si vous souhaitez comparer les résultats.

[Relatif : Comment assurer la sécurité de tous vos comptes dans un monde où les gens veulent vos données]

Google dispose également d'un vérificateur de mot de passe en ligne, mais il analyse les mots de passe que vous avez enregistrés sur votre compte Google via Chrome et Android - vous ne pouvez pas tester n'importe quel mot de passe avec.

Il vous avertira également des mots de passe que vous avez réutilisés alors que vous n'auriez pas dû, ainsi que des mots de passe inclus dans les fuites de violation de données.



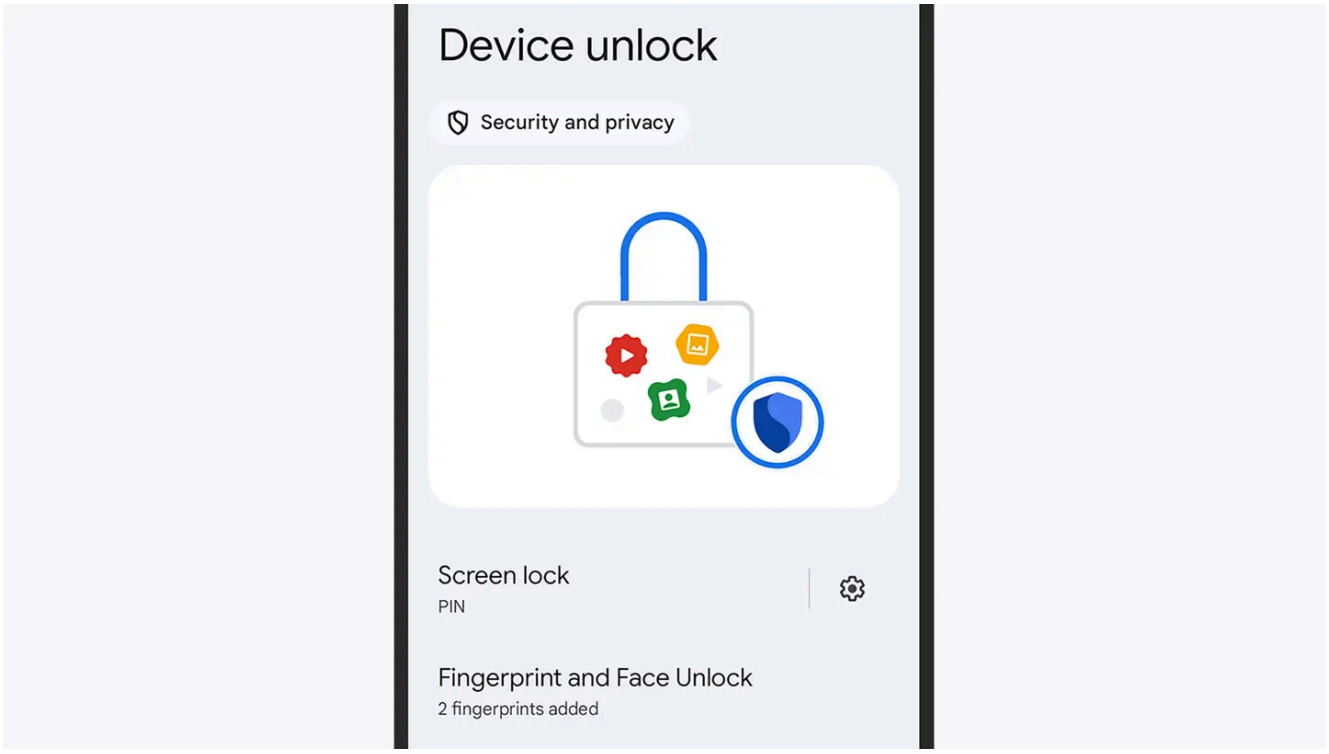
Capture d'écran : Gestionnaire de mots de passe

Si vous utilisez iCloud pour stocker vos mots de passe sur des appareils Apple, vous pouvez vérifier la sécurité de vos mots de passe via un iPhone, un iPad ou un Mac.
Sur l'iPhone, par exemple, dirigez-vous vers Paramètres, puis ouvrez **Mots de passe** et appuyez sur **Recommandations de sécurité** en haut.
Comme avec l'outil de Google, vous serez averti des mots de passe faibles, réutilisés et divulgués.

Ceux d'entre vous qui utilisent un gestionnaire de mots de passe devraient également trouver quelque chose de similaire dans votre logiciel.
Le populaire 1Password, par exemple, dispose d'une fonctionnalité appelée Watchtower : elle vous avertira si vos mots de passe ne sont pas assez forts, s'ils sont liés à des sites Web compromis ou s'ils ont été utilisés plusieurs fois.

Tous les gestionnaires de mots de passe, y compris ceux proposés par Google, Apple et 1Password, devraient être en mesure de générer des mots de passe aléatoires et forts en votre nom.
Ces mots de passe seront très difficiles à déchiffrer, et comme vous utilisez une application pour vous les souvenir tous, vous n'avez pas à vous soucier d'oublier ce qu'ils sont.

Comment protéger vos mots de passe



Assurez la protection de vos appareils.
Capture d'écran : Google

Vos mots de passe doivent être conservés en toute sécurité, et comme nous l'avons déjà mentionné, utiliser les services d'un gestionnaire de mots de passe est un bon début. L'utilisation de l'un de ces outils ne signifie pas que vous pouvez vous reposer sur vos lauriers : vous devez vous assurer que personne d'autre n'a accès à votre gestionnaire de mots de passe, ce qui leur donnerait alors accès à tous vos identifiants de connexion.

Cela signifie généralement verrouiller l'accès aux appareils sur lesquels vos gestionnaires de mots de passe sont en cours d'exécution, de sorte que votre ordinateur et votre smartphone doivent tous deux être bien protégés avec leurs propres codes PIN et mots de passe (ou l'authentification biométrique, ce qui est encore mieux).
Assurez-vous que ces appareils ne sont jamais laissés sans surveillance et qu'ils sont toujours verrouillés lorsqu'ils ne sont pas utilisés.

[Relatif : 15 façons d'être plus sûr en ligne]

En plus de deviner vos mots de passe et de les forcer par la force, vous devez également penser à une autre escroquerie populaire : l'ingénierie sociale.
C'est là que vous serez amené à taper vos identifiants de connexion sur un faux site Web, ou à les donner à quelqu'un lors d'un appel téléphonique ou d'une conversation par message direct.

Tout d'abord, ne donnez jamais vos mots de passe à qui que ce soit, quelle que soit la situation – si quelqu'un vous le demande, il n'est pas légitime.
Pour ce qui est d'éviter les sites Web frauduleux, gardez votre logiciel de navigation à jour (ces navigateurs sont formés pour repérer les sites Web suspects) et évitez de suivre les liens dans votre boîte de réception à moins d'être sûr qu'ils sont dignes de confiance, si vous venez de demander une réinitialisation de mot de passe, par exemple.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240401
"C'est ensemble qu'on avance"