www.dashlane.com /blog/top-8-most-important-passwords-to-change

Top 8 des mots de passe les plus importants à changer

NDMC: J'utilise le gestionnaire de mots de passe Dashlane depuis des années et je le recommande.
Dashlane :

Les mots de passe de nos ordinateurs et de nos appareils sécurisent tout, des informations bancaires et des numéros de sécurité sociale aux relevés de notes universitaires et aux messages privés.
Nous pourrions supposer que nos mots de passe les plus importants devraient être changés régulièrement, mais de bonnes habitudes de mot de passe et les gestionnaires de mots de passe réécrivent le livre de mots de passe.

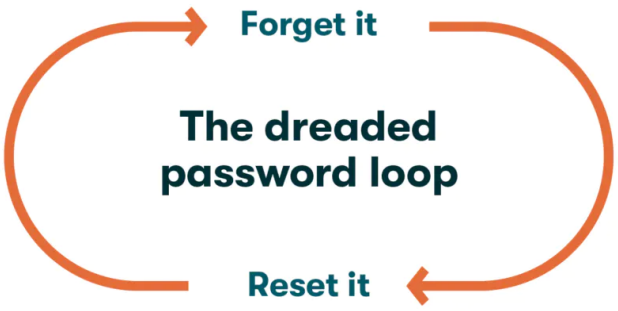
Risques liés à la sécurité des mots de passe pour 2023

La création, le stockage et la mémorisation des mots de passe sont devenus plus difficiles et plus critiques en même temps.
Il y a cinq raisons principales à cela :

1. **Plus de comptes et de mots de passe que jamais :**
   Avec la personne moyenne maintenant maintenant 70 à 80 mots de passe, il est devenu trop difficile de créer et de mémoriser *systématiquement autant* de mots de passe.
   Cela a conduit à une légère augmentation des mauvaises habitudes comme la réutilisation de mots de passe existants, la création de mots de passe très similaires et le stockage de mots de passe sur des blocs-notes et dans des fichiers numériques.
2. **Utilisation de divers appareils:**
   Le volume de comptes et de mots de passe a été aggravé par l'utilisation de plusieurs appareils, y compris les téléphones cellulaires, les ordinateurs portables et les tablettes qui doivent tous être sécurisés.
   Lorsque des appareils personnels sont utilisés pour des tâches professionnelles, les données de l'entreprise peuvent être exposées à davantage de risques de sécurité.
3. **Travail à distance et voyages :**
   Nos applications et nos comptes sont maintenant transportés avec nous partout où nous allons, ce qui rend les mots de passe plus vulnérables aux regards indiscrets ou aux cybercriminels qui comptent sur des réseaux WiFi privés non sécurisés pour intercepter des données.

Un VPN (réseau privé virtuel) protège les travailleurs à domicile et les voyageurs dans les lieux publics en acheminant et en cryptant toutes les données entrantes et sortantes via un portail sécurisé.

4. **Cyberattaques :**
   Les courriels d'hameçonnage qui nous incitent à cliquer sur des liens dangereux, les logiciels malveillants conçus pour perturber le fonctionnement normal de l'ordinateur et les tactiques d'enregistrement de frappe qui enregistrent nos frappes au clavier font partie des techniques de piratage destinées à compromettre la sécurité des mots de passe.
   Ces attaques néfastes continuent de devenir plus fréquentes chaque année à mesure que de plus en plus de nos informations d'identification se retrouvent sur la liste des mots de passe piratés d'un escroc, qui peuvent être vendues sur le Web sombre.
5. **Mots de passe non protégés :**
   Écrire des mots de passe sur un Post-It ou les enregistrer dans un document sur votre ordinateur les laisse sans protection.
   Oublier et réinitialiser constamment vos mots de passe est pénible, et si quelqu'un accède à l'e-mail que vous utilisez pour réinitialiser les mots de passe, il a la clé pour déverrouiller tous vos comptes en ligne.
   De tous les outils développés pour protéger les mots de passe, en particulier dans le contexte de la recrudescence des cyberattaques, les gestionnaires de mots de passe se démarquent.
   Ils génèrent, chiffrent, stockent et remplissent automatiquement les mots de passe afin que vous n'ayez pas à le faire, offrant sécurité, efficacité et commodité.



Vous souhaitez en savoir plus sur l'utilisation d'un gestionnaire de mots de passe ?

Consultez nos plans personnels ou commencez avec un essai gratuit.

3 raisons de *ne pas* changer de mot de passe régulièrement

Les réinitialisations obligatoires et périodiques des mots de passe ont conditionné beaucoup d'entre nous à croire que le simple fait de changer un mot de passe est le meilleur moyen de le rendre plus sûr, mais ce n'est pas toujours le cas.
Les changements de mot de passe forcés ou précipités peuvent en fait avoir l'effet inverse en raison de:

- **Mots de passe similaires :**
  Nous n'apportons souvent que des modifications mineures aux mots de passe existants, mettant à jour un ou deux caractères à la hâte.
  Selon le NIST, ces changements mineurs ne font pas grand-chose pour améliorer la sécurité puisque les attaquants par force brute sont conscients de cette pratique.
- **Réutilisation du mot de passe :**
  La réutilisation des mots de passe est une autre réponse naturelle aux changements forcés de mot de passe et à la surcharge du compte.
  Après tout, il est plus facile de se souvenir d'un mot de passe que de 100.
  Cette habitude met de nombreux comptes en danger car ils peuvent tous être compromis si ce mot de passe est braconné.
- **Temps perdu :**
  Changer fréquemment de mot de passe et essayer de se souvenir de tous vos nouveaux peut être un tracas fastidieux qui s'additionne vraiment.

Cela peut également conduire à des habitudes de stockage de mots de passe moins sécurisées, comme noter de nouveaux mots de passe dans un ordinateur portable afin de les avoir à portée de main pour la prochaine fois.

3 raisons de changer vos mots de passe au besoin

Vous demandez-vous comment changer tous vos mots de passe pour des mots de passe plus sécurisés?
Bien qu'il ne soit plus recommandé de changer *régulièrement* vos mots de passe, il existe des cas où la création d'un nouveau mot de passe est une sage décision:

- **Une entreprise avec laquelle vous avez un compte subit un piratage ou une violation :**
  Que vous entendiez parler du piratage ou de la violation dans les nouvelles ou que l'organisation vous contacte directement, l'option la plus sûre consiste à changer immédiatement le mot de passe du compte concerné.
  Assurez-vous qu'il est long, complexe et aléatoire, et qu'il n'a rien à voir avec votre ancien mot de passe.
- **Vous partagez un compte avec une personne qui se livre à des pratiques de mot de passe non sécurisées :**
  Si vous partagez un compte professionnel avec un collègue, tel que Twitter, ou un compte personnel avec votre famille et vos amis, tel qu'un service de streaming, la gestion sécurisée des mots de passe est encore plus importante.
  Si vous pensez que quelqu'un a partagé ou stocké de manière non sécurisée un mot de passe pour l'un de vos comptes, il est préférable de mettre à jour le mot de passe et d'en informer les autres utilisateurs du compte.
- **Votre mot de passe est faible :**
  Si l'un de vos mots de passe n'est pas long, aléatoire et complexe, il est considéré comme faible.
  Cela les rend plus faciles à deviner et à voler. Changer tous les mots de passe faibles protégera vos comptes en ligne contre les cybercriminels.

Vous voulez augmenter la force globale de votre mot de passe ? Obtenez cinq conseils d'experts.

Top 8 des mots de passe les plus importants à changer

Si beaucoup de vos mots de passe sont faibles et doivent être mis à jour, il peut être difficile de savoir par où commencer.
Pour vous faciliter la tâche, voici les mots de passe les plus importants à changer en premier :

1. **Messagerie électronique**

Bon nombre de vos mots de passe les plus critiques sont également parmi les plus anciens et les moins fréquemment modifiés, et les mots de passe de messagerie ne font pas exception.
Ces mots de passe ne fournissent pas d'accès *direct* aux informations financières, mais en tant qu'option 2FA, ils créent un chemin vers d'autres comptes importants.
En d'autres termes, un intrus peut utiliser un compte de messagerie pour déverrouiller systématiquement de nombreux comptes.
Heureusement, l'application Dashlane Authenticator remplace les codes envoyés par e-mail par des jetons rotatifs pour sécuriser les comptes compatibles avec 2FA.

D'autres actions dangereuses et indésirables pouvant résulter de mots de passe de messagerie perdus ou volés incluent les logiciels malveillants ou les spams envoyés à votre liste de contacts et les informations personnelles extraites de vos messages électroniques précédents.

2. **Activité bancaire**

Si vous avez subi des frais frauduleux sur votre carte de débit ou de crédit, mais que vous n'avez pas réussi à mettre à jour le mot de passe en ligne associé au compte, vous n'êtes pas seul.
Les mots de passe des comptes bancaires et de carte de crédit peuvent également stagner, ce qui peut être dangereux lorsqu'ils consistent en des phrases courantes et simples ou des informations personnelles telles que les noms et les dates de naissance. De nombreuses institutions financières ont pris des mesures proactives pour protéger la sécurité des mots de passe de leurs clients en mettant en œuvre 2FA et en augmentant le nombre minimum de caractères de mot de passe.

3. **Santé**

Les informations de santé telles que vos antécédents médicaux méritent également d'être traitées avec le plus grand respect de la confidentialité et de la sécurité des mots de passe.
En vertu de la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis, des directives pour la mise en œuvre de la 2FA,

la surveillance des tentatives de connexion et la modification, la création et la protection des mots de passe ont été créées pour protéger les droits à la vie privée des patients.
Si vous prenez rendez-vous ou vérifiez les résultats des tests à l'aide d'un portail en ligne, assurez-vous que votre mot de passe est sécurisé.

4. **Comptes professionnels**

Les mots de passe qui donnent accès à votre ordinateur de travail, à vos comptes professionnels et à vos systèmes sont souvent examinés et contrôlés de plus près par les employeurs, mais cela ne diminue pas leur risque ou leur importance.
Compte tenu des intervalles de réinitialisation des mots de passe préétablis dans de nombreuses entreprises, 54% des employés réutilisent des mots de passe sur plusieurs comptes professionnels.
De nombreuses entreprises utilisent des gestionnaires de mots de passe pour réduire les risques liés au travail à distance, au partage de mots de passe et au WiFi non sécurisé.

5. **Comptes scolaires**

Les mots de passe utilisés pour accéder aux cours et aux notes en ligne peuvent sembler moins critiques, mais entre de mauvaises mains, ces mots de passe peuvent exposer des informations personnelles telles que les numéros de sécurité sociale, les dates de naissance et les comptes de paiement.
Les écoles et les universités sont devenues des cibles de choix pour les cyberattaques, y compris les ransomwares, basées sur les énormes quantités de données précieuses qu'elles conservent et leur dépendance accrue à la communication virtuelle.

6. **Services de vente au détail et de streaming**

Tout comme les comptes bancaires ou de carte de crédit, les mots de passe des comptes de détail et de service d'abonnement peuvent fournir un accès direct à des informations financières confidentielles, ainsi qu'à d'autres identifiants tels que des numéros de téléphone et des adresses.
De nombreux mots de passe de comptes de vente au détail et de divertissement à domicile, tels que Netflix et Amazon, sont susceptibles d'être partagés avec des amis ou des membres de votre famille, ce qui augmente votre vulnérabilité si ces amis ou parents sont touchés par un cybercrime.

7. **Sites Web gouvernementaux**

Les services gouvernementaux et comptables, tels que l'IRS, conservent nos informations financières détaillées, ainsi que des identifiants importants tels que les numéros de sécurité sociale et les historiques d'adresses.
Heureusement, bon nombre de ces sites Web ont continué à renforcer les normes de cybersécurité en mettant en œuvre 2FA, des jetons et un cryptage pour réduire au minimum les réinitialisations de mot de passe.

8. **Applications de rencontres**

Les sites Web et les applications de rencontres sont également devenus des cibles pour les escrocs, les pirates informatiques et les imposteurs.
Tout comme les comptes scolaires, les services de rencontres capturent des informations confidentielles sur les clients telles que les dates et adresses de naissance, ainsi que des photos et des messages personnels.
Étant donné que de nombreuses applications de rencontres n'offrent pas de 2FA ou de cryptage, l'installation d'un gestionnaire de mots de passe est recommandée pour compléter votre confidentialité et votre sécurité en ligne.

Qu'est-ce qui rend un mot de passe sécurisé ?

Voici quelques directives supplémentaires que vous pouvez suivre pour améliorer considérablement l'hygiène de votre mot de passe :

- **Long, aléatoire et complexe :** *quelle doit être la longueur des mots de passe ?* Bien que le nombre de caractères soit important (12 est bien meilleur que 8), les caractères doivent également être un mélange de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux pour créer des mots de passe aléatoires et complexes.
  Les mots courants et les phrases ou chiffres personnels comme votre prénom, le nom de votre animal de compagnie ou votre année de naissance doivent être laissés de côté.
  Combien de temps faut-il pour pirater mon mot de passe?
  Cela dépend aussi de la longueur et de la complexité.

Le meilleur logiciel de piratage prendrait 34 000 ans pour déchiffrer un mot de passe de 12 caractères avec au moins une lettre majuscule, un symbole et un chiffre.

- **Non partagé de manière non sécurisée avec d'autres :**
  Le partage de mots de passe pour les comptes de vente au détail et de service de streaming est courant.
  Les mots de passe des applications en milieu de travail sont également partagés entre les employés.
  Si une personne avec qui vous avez partagé un mot de passe est touchée par un cybercrime, votre identité et vos informations deviennent également vulnérables.
  Dashlane fournit un portail chiffré pour le partage de mots de passe qui vous permet de transférer des informations de mot de passe en toute sécurité sans sacrifier la confidentialité ni augmenter la vulnérabilité.

- **Stockées en toute sécurité (et cryptées) :**
  Stocker les mots de passe dans un fichier numérique ou physique est l'option la moins sûre.
  Les stocker dans des gestionnaires de mots de passe de navigateur intégrés qui sauvegardent vos informations sur leurs serveurs n'est que légèrement plus sûr car ces gestionnaires de mots de passe de navigateur ne chiffrent pas vos mots de passe, ce qui les rend vulnérables en cas de violation.
  Les gestionnaires de mots de passe qui utilisent une architecture à connaissance nulle, comme Dashlane, sont plus sûrs car ils chiffrent et stockent vos données de mot de passe sur des serveurs cloud hébergés hautement sécurisés.

Comment Dashlane vous aide à sécuriser vos mots de passe

Le gestionnaire de mots de passe Dashlane vous permet de conserver tous vos mots de passe les plus importants dans une seule application sécurisée.
La génération et le chiffrement automatiques des mots de passe éliminent le besoin de créer, de mémoriser et de réinitialiser des mots de passe complexes pour chaque compte. La sécurité et l'efficacité s'améliorent à mesure que Dashlane crée, stocke et remplit automatiquement des mots de passe complexes et uniques pour vous.

Références

1. Rackspace, « Journée mondiale du mot de passe : conseils de sécurité des mots de passe d'un expert en cybersécurité », mai 2022.
2. Dashlane, « *How to Stop Reusing Passwords for Good* », janvier 2020.
3. Dashlane, *« Pourquoi chaque appareil d'employé devrait être sécurisé »,* mai 2021.
4. Dashlane, « *Pourquoi avez-vous besoin d'un VPN ? Ne manquez pas ces 3 avantages clés* », août 2020.
5. Security Magazine, « *Email cyberattacks increased 48% in first half of* 2022 », août 2022.
6. Dashlane, « *What the Hack is 2FA ?* » Janvier 2020.
7. Statista, « *Nombre annuel de compromissions de données et d'individus touchés aux États-Unis de 2005 au premier semestre* 2022 », août 2022.
8. NIST, « *Directives sur l'identité numérique* », 2022.

9. SI Partners, « *Security Surprise: Enforcing Regular Password Changes Puts Your Organization at Risk* », août 2022.
10. Dashlane, « *Quelle est la force de votre mot de passe et devriez-vous le changer ?* » Août 2022.
11. Dashlane, « *FAQ sur Dashlane Authenticator* », 2022.
12. Dashlane, « *10 mots de passe les plus courants (le vôtre figure-t-il sur la liste ?)* », septembre 2022.
13. HelpNet Security, « *54 % de tous les employés réutilisent les mots de passe sur plusieurs comptes professionnels* », juin 2021.
14. Dashlane, « *3 pratiques de sécurité du travail à distance pour votre petite entreprise* », octobre 2022.
15. Poynter, « *Le deuxième plus grand système scolaire du pays vient d'être touché par une cyberattaque. Pourquoi les attaquants ciblent-ils les écoles ?* Septembre 2022.
16. The Guardian, « *Cinq dilemmes d'applications de rencontres répondus par des experts* », juillet 2022.
17. HIPAA Journal, « *The HIPAA Password Requirements and the Best Way to Comply with Them* », juin 2022.
18. Forum économique mondial, « *Ce graphique montre combien de temps il faudrait à un ordinateur pour pirater votre mot de passe exact* », décembre 2021.
19. Dashlane, « *Une plongée profonde dans la sécurité Zero-Knowledge de Dashlane* », 2022.
20. Dashlane, « *Class is in Session with Dashlane's Worst Password Awards* », mai 2021.
21. Cybersecurity and Infrastructure Security Agency, « Executive Order on Improving the Nation's Cybersecurity », mai 2022.
22. Dashlane, « How to Erase Saved Browser Passwords: Step-by-Step Guide », novembre 2022.
23. Dashlane, « Qu'est-ce qu'une phrase secrète et comment puis-je en créer une ? » Novembre 2022.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230731
"C'est ensemble qu'on avance"