RESOURCE CENTER

Rapport sur l'état de la sécurité des mots de passe 2024

Comment les agences fédérales abordent la question de la sécurité des mots de passe

Get the full interactive view at
https://bitwarden.com/fr-fr/resources/the-state-of-password-security/

bitwarden

Évaluation de l'état de la sécurité des mots de passe dans les agences fédérales américaines

Ces dernières années, le gouvernement fédéral des États-Unis a mis l'accent sur la cybersécurité et de nombreuses agences ont pris l'initiative d'informer les organisations gouvernementales, les entreprises, grandes et petites, ainsi que les consommateurs.

Cependant, en ce qui concerne la sécurité des mots de passe, toutes les agences ne chantent pas la même chanson. L'un des groupes les plus importants, le National Institute of Standards and Technology (NIST), "élabore des normes, des lignes directrices, des meilleures pratiques et d'autres ressources en matière de cybersécurité pour répondre aux besoins de l'industrie américaine, des agences fédérales et du grand public".

La page du NIST consacrée à la cybersécurité précise que "certaines missions du NIST en matière de cybersécurité sont définies par des lois fédérales, des ordres exécutifs et des politiques. Par exemple, l'Office of Management and Budget (OMB) exige que toutes les agences fédérales mettent en œuvre les normes et les orientations du NIST en matière de cybersécurité pour les systèmes ne relevant pas de la sécurité nationale".

Malheureusement, les recommandations du NIST n'ont pas encore été universellement acceptées et mises en œuvre par toutes les agences fédérales. Et si le NIST établit les normes que les agences sont censées respecter, il a lui aussi ses propres faiblesses, sous la forme d'un site web désorganisé.

2024 marque la troisième année au cours de laquelle Bitwarden a effectué cette analyse. En trois ans, le site web du NIST est resté désorganisé, bien que son contenu soit très solide. Il y a également eu quelques développements positifs. La Maison Blanche a amélioré la diffusion des conseils en matière de sécurité des mots de passe, passant d'une note "perfectible" à une note "bonne". Parmi les autres agences qui ont amélioré leurs recommandations en matière de sécurité des mots de passe et leur position générale en matière de cybersécurité, on peut citer la Cybersecurity and Infrastructure Security Association (CISA), le Federal Bureau of Investigation (FBI), la Federal Trade Commission (FTC) et la Small Business Administration (SBA).

Cette année, Bitwarden a également ajouté la Securities and Exchange Commission (SEC) à ce rapport. L'année dernière, la SEC a adopté des règles exigeant que les entreprises divulguent les incidents importants liés à la cybersécurité. Étant donné le rôle de la SEC dans l'application de la conformité en matière de cybersécurité, ce rapport évaluera les conseils de la SEC en matière de sécurité des mots de passe.

La technologie évolue rapidement. Pour les entreprises et les particuliers, une grande partie de notre vie se déroule désormais en ligne, sur une myriade de comptes qui vont des sites de divertissement aux affaires financières sérieuses comme nos comptes bancaires.

L'objectif de cette évaluation est d'impliquer et d'éduquer toutes les personnes qui utilisent des mots de passe sur les meilleures pratiques du gouvernement fédéral et sur les points à améliorer. Au sein du gouvernement fédéral, nombreux sont ceux qui ont une solide approche éducative de la sécurité des mots de passe, tandis que d'autres ont besoin d'un peu d'aide pour se moderniser.

Heureusement, les meilleures pratiques en matière de sécurité des mots de passe font l'objet d'un consensus. Ce rapport consolide et évalue les détails.

The State of Password Security: How federal agencies are addressing password security

Download

Voir la présentation sur l'état de la sécurité des mots de passe Présentation sur l'état de la sécurité des mots de passe

Table des matières

Lignes directrices pour le système d'évaluation de la sécurité des mots de passe

Le système de notation classe les agences en fonction du respect des critères suivants :

Excellent

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité sont à jour et respectent les lignes directrices du NIST.
- présente les recommandations en matière de sécurité des mots de passe d'une manière claire, digeste et facile à trouver

Very Good

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité sont à jour et respectent les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Good

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Fair

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe

- Appel à l'importance de mots de passe forts
- ne mentionne pas systématiquement la nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Room for Improvement

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- N'insiste pas sur l'importance de mots de passe forts
- Ne mentionne pas le besoin de 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Institut national des normes et de la technologie (NIST)

Cadre de gestion des risques du NIST | IA-5(18)

Conseil de l'Agence :

- Authenticator Management | Gestionnaires de mots de passe
  - Employer [Affectation : gestionnaires de mots de passe définis par l'organisation] pour générer et gérer les mots de passe ; et
    - Protéger les mots de passe à l'aide de [affectation : contrôles définis par l'organisation].
    - Pour les systèmes utilisant des mots de passe statiques, il est souvent difficile de s'assurer que les mots de passe sont suffisamment complexes et que les mêmes mots de passe ne sont pas utilisés sur plusieurs systèmes. Un gestionnaire de mots de passe est une solution à ce problème car il génère et stocke automatiquement des mots de passe forts et différents pour différents comptes. Un risque potentiel lié à l'utilisation de gestionnaires de mots de passe est que des adversaires peuvent cibler la collection de mots de passe générés par le gestionnaire de mots de passe. Par conséquent, la collecte des mots de passe doit être protégée, notamment par le cryptage des mots de passe et le stockage hors ligne de la collection dans un jeton.

- Référence

Lignes directrices sur l'identité numérique

Conseil de l'Agence :

- Les secrets mémorisés DOIVENT comporter au moins 8 caractères s'ils sont choisis par l'abonné. Les secrets mémorisés choisis au hasard par le CSP ou le vérificateur DOIVENT comporter au moins 6 caractères et PEUVENT être entièrement numériques. Si le CSP ou le vérificateur refuse un secret mémorisé choisi parce qu'il figure sur une liste noire de valeurs compromises, l'abonné DOIT être tenu de choisir un autre secret mémorisé. Aucune autre exigence de complexité ne devrait être imposée pour les secrets mémorisés. Une justification de ce choix est présentée à l'annexe A - Force des secrets mémorisés.

- Les vérificateurs DOIVENT exiger que les secrets mémorisés choisis par l'abonné comportent au moins 8 caractères. Les vérificateurs DEVRAIENT autoriser les secrets mémorisés choisis par l'abonné, d'une longueur d'au moins 64 caractères. Tous les caractères d'impression ASCII [RFC 20] ainsi que le caractère espace DEVRAIENT être acceptés dans les secrets mémorisés. Les caractères Unicode [ISO/ISC 10646] DEVRAIENT également être acceptés. Pour tenir compte des risques d'erreur de frappe, les vérificateurs PEUVENT remplacer plusieurs caractères d'espacement consécutifs par un seul caractère d'espacement avant la vérification, à condition que le résultat ait une longueur d'au moins 8 caractères. La troncature du secret NE DOIT PAS être effectuée. Aux fins des exigences de longueur ci-dessus, chaque point de code Unicode DOIT être considéré comme un seul caractère.

- Les secrets mémorisés qui sont choisis de manière aléatoire par le CSP (par exemple, lors de l'inscription) ou par le vérificateur (par exemple, lorsqu'un utilisateur demande un nouveau code PIN) DOIVENT comporter au moins 6 caractères et DOIVENT être générés à l'aide d'un générateur de bits aléatoires approuvé [SP 800-90Ar1].

- Les vérificateurs de secrets mémorisés NE DOIVENT PAS permettre à l'abonné de stocker un "indice" accessible à un demandeur non authentifié. Les vérificateurs NE DOIVENT PAS inviter les abonnés à utiliser des types d'informations spécifiques (par exemple, "Quel était le nom de votre premier animal de compagnie ?") lorsqu'ils choisissent des secrets mémorisés.

- Lorsqu'ils traitent des demandes d'établissement et de modification de secrets mémorisés, les vérificateurs DOIVENT comparer les secrets potentiels à une liste contenant des valeurs connues pour être couramment utilisées, attendues ou compromises. Par exemple, la liste PEUT comprendre, sans s'y limiter, les éléments suivants :
  - Mots de passe obtenus à partir de corpus de violations antérieurs.
  - Mots du dictionnaire.
  - Caractères répétitifs ou séquentiels (par exemple, "aaaaaa", "1234abcd").
  - Les mots spécifiques au contexte, tels que le nom du service, le nom d'utilisateur et leurs dérivés.

- Si le secret choisi se trouve dans la liste, le CSP ou le vérificateur DOIT informer l'abonné qu'il doit choisir un autre secret, indiquer la raison du rejet et demander à l'abonné de choisir une autre valeur.

- Les vérificateurs DEVRAIENT offrir des conseils à l'abonné, tels qu'un compteur de force de mot de passe [Meters], afin d'aider l'utilisateur à choisir un secret mémorisé fort. Ceci est particulièrement important après le rejet d'un secret mémorisé sur la liste ci-dessus, car cela décourage la modification triviale de secrets mémorisés répertoriés (et probablement très faibles) [Listes noires].

- Les vérificateurs DOIVENT mettre en œuvre un mécanisme de limitation du taux qui limite effectivement le nombre de tentatives d'authentification infructueuses qui peuvent être effectuées sur le compte de l'abonné, comme décrit à la section 5.2.2.

- Les vérificateurs NE DOIVENT PAS imposer d'autres règles de composition (par exemple, exiger des mélanges de différents types de caractères ou interdire les caractères répétés consécutivement) pour les secrets mémorisés. Les vérificateurs NE DOIVENT PAS exiger que les secrets mémorisés soient modifiés arbitrairement (par exemple, périodiquement). Toutefois, les vérificateurs DOIVENT imposer un changement s'il existe des preuves de la compromission de l'authentificateur.

- Les vérificateurs DEVRAIENT permettre aux demandeurs d'utiliser la fonction "coller" lors de la saisie d'un secret mémorisé. Cela facilite l'utilisation des gestionnaires de mots de passe, qui sont largement utilisés et qui, dans de nombreux cas, augmentent la probabilité que les utilisateurs choisissent des secrets mémorisés plus forts.

- Afin d'aider le demandeur à saisir avec succès un secret mémorisé, l'organisme vérificateur DEVRAIT offrir la possibilité d'afficher le secret - plutôt qu'une série de points ou d'astérisques - jusqu'à ce qu'il soit saisi. Cela permet au demandeur de vérifier son entrée s'il se trouve dans un endroit où son écran a peu de chances d'être observé. Le vérificateur PEUT également permettre à l'appareil de l'utilisateur d'afficher les caractères individuels saisis pendant une courte période après la frappe de chaque caractère afin de vérifier que la saisie est correcte. Ceci est particulièrement vrai pour les appareils mobiles.

- Le vérificateur DOIT utiliser un chiffrement approuvé et un canal protégé authentifié lorsqu'il demande des secrets mémorisés afin d'assurer une résistance à l'écoute et aux attaques MitM.

- Les vérificateurs DOIVENT stocker les secrets mémorisés sous une forme qui résiste aux attaques hors ligne. Les secrets mémorisés DOIVENT être salés et hachés à l'aide d'une fonction de dérivation de clé à sens unique appropriée. Les fonctions de dérivation de clé prennent en entrée un mot de passe, un sel et un facteur de coût, puis génèrent un hachage du mot de passe. Leur objectif est de rendre coûteux chaque essai de devinette de mot de passe par un attaquant qui a obtenu un fichier de hachage de mot de passe et, par conséquent, le coût d'une attaque de devinette élevé ou prohibitif. Parmi les exemples de fonctions de dérivation de clés appropriées, on peut citer Password-based Key Derivation Function 2 (PBKDF2) [SP 800-132] et Balloon [BALLOON]. Une fonction à mémoire dure DEVRAIT être utilisée car elle augmente le coût d'une attaque. La fonction de dérivation de clé DOIT utiliser une fonction à sens unique approuvée telle que Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], toute fonction de hachage approuvée dans la SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] ou Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE), ou ParallelHash [SP 800-185]. La longueur de sortie choisie de la fonction de dérivation de clé DEVRAIT être la même que la longueur de sortie de la fonction à sens unique sous-jacente.

- Le sel DOIT avoir une longueur d'au moins 32 bits et être choisi arbitrairement de manière à minimiser les collisions de valeurs de sel entre les hachages stockés. La valeur du sel et le hachage qui en résulte DOIVENT être stockés pour chaque abonné à l'aide d'un authentificateur secret mémorisé.

- Pour PBKDF2, le facteur de coût est le nombre d'itérations : plus la fonction PBKDF2 est itérée, plus il faut de temps pour calculer le hachage du mot de passe. Par conséquent, le nombre d'itérations DEVRAIT être aussi élevé que le permettent les performances du serveur de vérification, en général au moins 10 000 itérations.

- En outre, les vérificateurs DEVRAIENT effectuer une itération supplémentaire d'une fonction de dérivation de clé à l'aide d'une valeur de sel secrète et connue uniquement du vérificateur. Cette valeur saline, si elle est utilisée, DOIT être générée par un générateur de bits aléatoires approuvé [SP 800-90Ar1] et fournir au moins la force de sécurité minimale spécifiée dans la dernière révision de SP 800-131A (112 bits à la date de la présente publication). La valeur saline secrète DOIT être stockée séparément des secrets mémorisés hachés (par exemple, dans un dispositif spécialisé tel qu'un module de sécurité matériel). Avec cette itération supplémentaire, les attaques par force brute sur les secrets mémorisés hachés sont impossibles tant que la valeur saline secrète reste secrète.

- Série de blogs sur le Mois de la sensibilisation à la cybersécurité 2023
  - Conseil de l'Agence
    - Les mots de passe restent le mécanisme d'authentification le plus utilisé pour accéder à des ressources intéressantes. Les mots de passe constituent la première ligne de défense pour protéger la confidentialité et l'intégrité des données contre les cybercriminels et les violations de données. Des mots de passe efficaces et robustes permettent aux internautes de rester en sécurité et de préserver leur vie privée en ligne.

- Référence

bitwarden

Institut national des normes et de la technologie (NIST)

Évaluation globale du Bitwarden : Très bon

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils en matière de sécurité sont actualisés et respectent les lignes directrices du NIST (le NIST définit la norme pour les conseils en matière de sécurité du gouvernement fédéral).
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

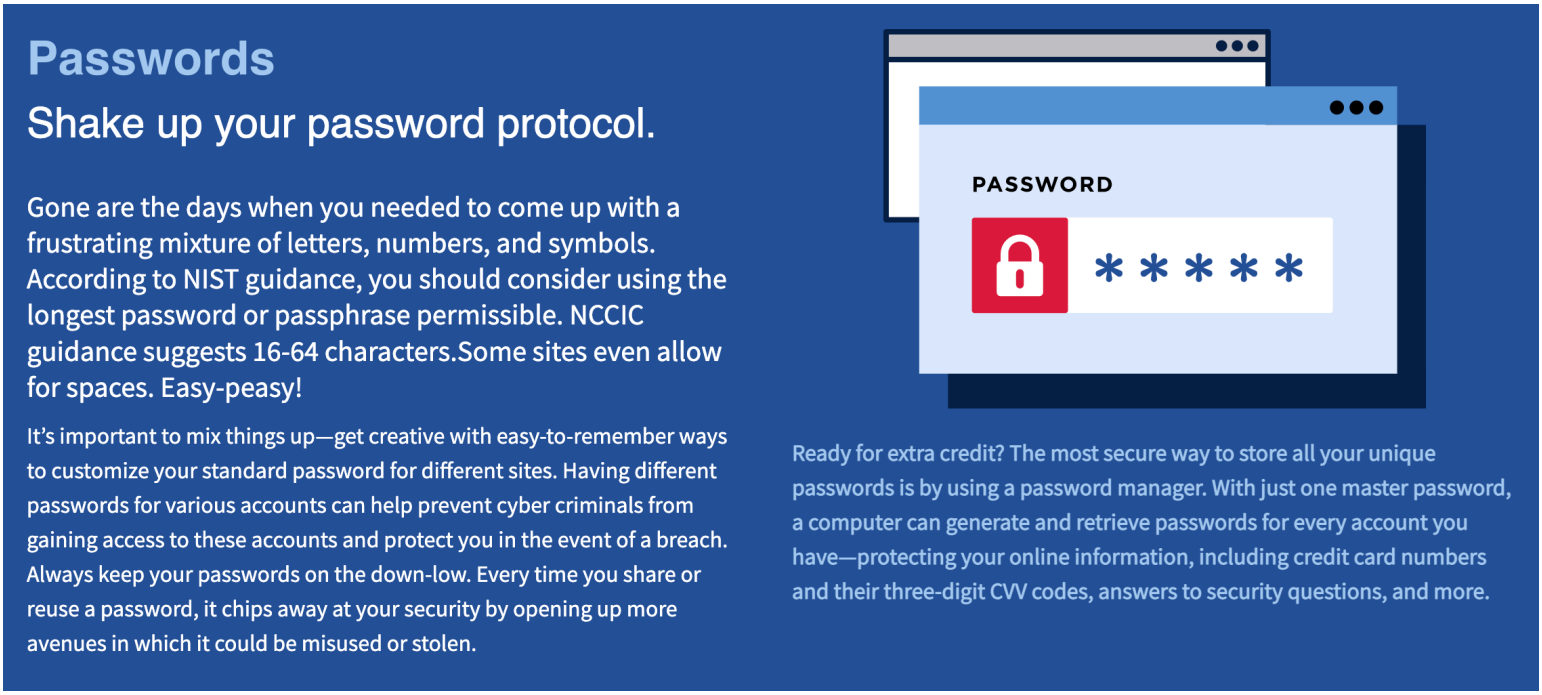
Bien que les conseils soient complets et fixent les normes pour les agences, l'accès aux lignes directrices sur les mots de passe via le site web n'est pas intuitif. Les conseils sont noyés dans des PDF très longs et rédigés d'une manière peu conviviale.

"Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

NIST

Agence pour la cybersécurité et la sécurité des infrastructures (CISA)

Leçons sur le cyberespace



Leçons de cybernétique sur les mots de passe, CISA

- Référence

Guide pour arrêter les ransomwares

Conseil de l'Agence :

- Mettre en œuvre des politiques de mots de passe qui exigent des mots de passe uniques d'au moins 15 caractères.
  - Les gestionnaires de mots de passe peuvent vous aider à élaborer et à gérer des mots de passe sécurisés. Sécuriser et limiter l'accès à tout gestionnaire de mot de passe utilisé et activer toutes les fonctions de sécurité disponibles sur le produit utilisé, telles que l'AMF.

- Référence

Sécuriser notre monde : Exiger des mots de passe forts

Conseil de l'Agence :

- Les petites et moyennes entreprises sont régulièrement la cible de pirates informatiques malveillants et l'un des points d'entrée les plus courants pour les voleurs numériques est le vol ou la faiblesse des mots de passe.

- Mais la bonne nouvelle, c'est que vous pouvez assurer la sécurité de votre entreprise en demandant à vos employés d'utiliser des mots de passe forts et des gestionnaires de mots de passe.

- Montrez l'exemple en utilisant des mots de passe longs, aléatoires et uniques pour tous vos comptes personnels et professionnels, et utilisez un gestionnaire de mots de passe pour vous en souvenir ! Travaillez ensuite avec votre personnel informatique ou votre fournisseur pour exiger des employés qu'ils utilisent des mots de passe forts pour accéder à vos systèmes. Vos données seront ainsi protégées et sécurisées.

- Référence

Sécuriser notre monde : Mots de passe faibles

Conseil de l'Agence :

- Laissez un gestionnaire de mots de passe faire le travail ! Un gestionnaire de mots de passe crée, stocke et remplit automatiquement les mots de passe pour nous. Nous n'aurons alors plus qu'à nous souvenir d'un seul mot de passe fort - pour le gestionnaire de mots de passe lui-même. Recherchez des sources fiables pour les "gestionnaires de mots de passe", comme Consumer Reports, qui propose une sélection de gestionnaires de mots de passe très bien notés. Lisez les commentaires pour comparer les options et trouver un programme réputé pour vous.

- Référence

bitwarden

Agence pour la cybersécurité et la sécurité des infrastructures (CISA)

Appréciation globale du Bitwarden : Très bon

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité sont à jour et respectent les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

L'Agence nationale de sécurité (NSA)

Guide pour arrêter les ransomwares

Conseil de l'Agence :

- Mettre en œuvre des politiques de mots de passe qui exigent des mots de passe uniques d'au moins 15 caractères.
  - Les gestionnaires de mots de passe peuvent vous aider à élaborer et à gérer des mots de passe sécurisés. Sécuriser et limiter l'accès à tout gestionnaire de mot de passe utilisé et activer toutes les fonctions de sécurité disponibles sur le produit utilisé, telles que l'AMF.
- Référence

Types de mots de passe Cisco : Meilleures pratiques

Conseil de l'Agence :

- L'augmentation du nombre de compromissions d'infrastructures de réseau ces dernières années nous rappelle que l'authentification des dispositifs de réseau est un élément important. Les dispositifs du réseau peuvent être compromis en raison de :
  - Mauvais choix de mot de passe (vulnérable à la pulvérisation de mot de passe par force brute)
  - les fichiers de configuration du routeur (qui contiennent des mots de passe hachés) envoyés par courrier électronique non crypté, ou
  - Les mots de passe réutilisés (lorsque les mots de passe récupérés sur un appareil compromis peuvent être utilisés pour compromettre d'autres appareils).
- L'utilisation de mots de passe seuls augmente le risque d'exploitation du dispositif. Bien que la NSA recommande vivement l'authentification multifactorielle pour les administrateurs gérant des dispositifs critiques, il faut parfois se contenter de mots de passe. Le choix de bons algorithmes de stockage des mots de passe peut rendre l'exploitation beaucoup plus difficile.
- Pour assurer une protection maximale, utilisez des mots de passe forts afin d'éviter qu'ils ne soient déchiffrés et convertis en texte clair. Se conformer à une politique de mot de passe qui :

- Il s'agit d'une combinaison de lettres minuscules et majuscules, de symboles et de chiffres ;
- comporte au moins 15 caractères alphanumériques ; et
- Les modèles qui ne le sont pas :
  - Une promenade au clavier
  - Identique à un nom d'utilisateur
  - Le mot de passe par défaut
  - Identique à un mot de passe utilisé ailleurs
  - Relatif au réseau, à l'organisation, à la localisation ou à d'autres identifiants de fonction
  - Directement à partir d'un dictionnaire, d'acronymes courants ou faciles à deviner

- Référence

La sécurité sur les médias sociaux

Conseil de l'Agence :

- Sécurisez et renforcez vos mots de passe
  - Utilisez des mots de passe uniques et robustes pour chaque compte en ligne. La réutilisation de mots de passe sur plusieurs comptes peut exposer les données de tous les comptes si le mot de passe est découvert. Veillez à ce que votre mot de passe soit suffisamment long et complexe, en utilisant une combinaison de lettres, de chiffres et de caractères spéciaux. Dans la mesure du possible, mettez en place une authentification multifactorielle à l'aide d'un jeton d'authentification ou d'une application afin que personne ne puisse accéder à votre compte même si votre mot de passe est compromis. Ne partagez jamais vos mots de passe et évitez d'utiliser des informations qui pourraient être devinées à partir de vos profils de médias sociaux ou d'informations publiques.

- Référence

Sélection de solutions d'authentification multi-facteurs sécurisées

Conseil de l'Agence :

- Les mécanismes d'authentification multifactorielle à réponse unique nécessitent l'activation du dispositif, soit par un code PIN/mot de passe, soit par des données biométriques. Le dispositif fournit "ce que vous avez" et l'activation du dispositif implique que "ce que vous savez" ou "ce que vous êtes" a été vérifié.

- D'autre part, les authentificateurs en plusieurs étapes comprennent souvent un mot de passe qui fournit "ce que vous savez" et un autre authentificateur qui fournit "ce que vous avez". Les agences gouvernementales américaines devraient envisager des exigences pour l'activation des codes PIN/mots de passe ainsi que pour les mots de passe qui sont utilisés directement pour fournir "ce que vous savez". Les lignes directrices du SP 800-63-3, partie B, indiquent que les secrets mémorisés (à la fois pour l'activation et en tant qu'authentificateur à facteur unique) doivent comporter au moins 6 à 8 caractères, et recommandent une force de mot de passe plus élevée pour les mots de passe sélectionnés par l'utilisateur. Lors de la détermination des exigences en matière de mot de passe, il convient de noter que les dispositifs multifacteurs doivent intégrer des seuils stricts pour lutter contre les attaques par devinette de mot de passe, tandis que les vérificateurs peuvent utiliser des mécanismes de seuil moins stricts qui justifient que les mots de passe utilisés directement aient des exigences plus élevées en matière de force.

- Référence

Very Good

bitwarden

L'Agence nationale de sécurité (NSA)

Évaluation globale du Bitwarden : Bonne

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

"Disable the feature that allows web browsers to remember your passwords. Secure your passwords in a password manager."

NSA

Département de la sécurité intérieure

La loi CISA relève du DHS

Page sur la cybersécurité

Conseil de l'Agence :

- Le président Biden a fait de la cybersécurité, un élément essentiel de la mission du ministère de la sécurité intérieure (DHS), une priorité absolue de l'administration Biden-Harris à tous les niveaux du gouvernement.
- Afin de concrétiser l'engagement du président et de montrer que le renforcement de la résilience de la nation en matière de cybersécurité est une priorité absolue pour le ministère de la sécurité intérieure, le secrétaire Mayorkas a lancé un appel à l'action consacré à la cybersécurité au cours du premier mois de son mandat. Cet appel à l'action se concentre sur la lutte contre la menace immédiate des ransomwares et sur la mise en place d'une main-d'œuvre plus solide et plus diversifiée.
- En mars 2021, le secrétaire d'État Mayorkas a présenté sa vision élargie et une feuille de route pour les efforts du ministère en matière de cybersécurité lors d'un discours virtuel organisé par RSA Conference, en partenariat avec l'université de Hampton et les Girl Scouts of the USA.
- Après sa présentation, le secrétaire d'État a été rejoint par Judith Batty, directrice générale par intérim des Girls Scouts, pour une discussion au coin du feu sur les défis sans précédent auxquels les États-Unis sont actuellement confrontés en matière de cybersécurité. Chutima Boonthum-Denecke, du département d'informatique de l'université de Hampton, a présenté la secrétaire et a animé une séance de questions-réponses pour clore le programme.
  - Vue d'ensemble des sprints de cybersécurité du DHS

Room for Improvement

bitwarden

Département de la sécurité intérieure

Évaluation globale du Bitwarden : Une marge d'amélioration

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- N'insiste pas sur l'importance de mots de passe forts
  - offre des conseils inexacts et malavisés en matière de sécurité des mots de passe OU ne mentionne pas les mots de passe ou la sécurité des mots de passe
  - N'indique pas clairement les conseils relatifs au mot de passe
- ne mentionne pas systématiquement la nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Bureau fédéral d'enquête (FBI)

La cybermenace

Conseil de l'Agence :

- Les délits et les cyberintrusions liés à l'internet deviennent de plus en plus sophistiqués et leur prévention exige que chaque utilisateur d'un appareil connecté soit conscient et sur ses gardes.
- Maintenez les systèmes et les logiciels à jour et installez un programme antivirus puissant et réputé.
- Soyez prudent lorsque vous vous connectez à un réseau Wi-Fi public et n'effectuez aucune transaction sensible, y compris des achats, lorsque vous êtes sur un réseau public.
- Créez une phrase de passe forte et unique pour chaque compte en ligne et modifiez-la régulièrement.
- Mettez en place l'authentification multifactorielle sur tous les comptes qui le permettent.
- Examinez l'adresse électronique dans toute correspondance et vérifiez les URL des sites web avant de répondre à un message ou de visiter un site.
- Ne cliquez pas sur les messages électroniques ou textuels non sollicités.
- Soyez prudent quant aux informations que vous partagez dans les profils en ligne et les comptes de médias sociaux. Le fait de donner des noms d'animaux, d'écoles et de membres de la famille peut donner aux escrocs les indices dont ils ont besoin pour deviner vos mots de passe ou les réponses aux questions de sécurité de votre compte.
- N'envoyez pas de paiements à des personnes ou à des organisations inconnues qui cherchent à obtenir un soutien financier et qui demandent une action immédiate.

- Référence

Escroqueries et sécurité sur Internet

Conseil de l'Agence :

- **Gardez votre pare-feu activé**

  Un pare-feu permet de protéger votre ordinateur contre les pirates qui pourraient essayer d'y accéder pour le planter, supprimer des informations ou même voler des mots de passe ou d'autres informations sensibles. Les pare-feu logiciels sont largement recommandés pour les ordinateurs individuels. Le logiciel est préinstallé sur certains systèmes d'exploitation ou peut être acheté pour des ordinateurs individuels. Pour plusieurs ordinateurs en réseau, les routeurs matériels fournissent généralement une protection par pare-feu.

- **Installez ou mettez à jour votre logiciel antivirus**

  Les logiciels antivirus sont conçus pour empêcher les programmes malveillants de s'installer sur votre ordinateur. S'il détecte un code malveillant, tel qu'un virus ou un ver, il s'efforce de le désarmer ou de le supprimer. Les virus peuvent infecter les ordinateurs à l'insu des utilisateurs. La plupart des logiciels antivirus peuvent être configurés pour se mettre à jour automatiquement.

- **Installez ou mettez à jour votre technologie antispyware**

  Les logiciels espions sont exactement ce qu'ils semblent être : des logiciels installés subrepticement sur votre ordinateur pour permettre à d'autres personnes d'observer vos activités sur l'ordinateur. Certains logiciels espions collectent des informations sur vous sans votre consentement ou produisent des fenêtres publicitaires intempestives sur votre navigateur web. Certains systèmes d'exploitation offrent une protection gratuite contre les logiciels espions, et des logiciels peu coûteux peuvent être téléchargés sur Internet ou dans votre magasin d'informatique. Méfiez-vous des publicités sur Internet proposant des logiciels anti-spyware téléchargeables. Dans certains cas, ces produits peuvent être faux et contenir des logiciels espions ou d'autres codes malveillants. C'est comme pour l'épicerie : faites vos courses là où vous avez confiance.

- **Maintenez votre système d'exploitation à jour**

  Les systèmes d'exploitation informatiques sont périodiquement mis à jour afin de rester en phase avec les exigences technologiques et de corriger les failles de sécurité. Veillez à installer les mises à jour pour vous assurer que votre ordinateur dispose de la protection la plus récente.

- **Faites attention à ce que vous téléchargez**

  Le téléchargement inconsidéré de pièces jointes à des courriels peut contourner même les logiciels antivirus les plus vigilants. N'ouvrez jamais une pièce jointe à un courriel provenant d'une personne que vous ne connaissez pas et méfiez-vous des pièces jointes transférées par des personnes que vous connaissez. Ils peuvent avoir involontairement avancé un code malveillant.

- **Éteignez votre ordinateur**

  Avec le développement des connexions Internet à haut débit, nombreux sont ceux qui choisissent de laisser leur ordinateur allumé et prêt à l'emploi. L'inconvénient est que le fait d'être "toujours allumé" rend les ordinateurs plus vulnérables. Au-delà de la protection par pare-feu, qui est conçue pour repousser les attaques indésirables, la mise hors tension de l'ordinateur permet de couper la connexion d'un attaquant, qu'il s'agisse d'un logiciel espion ou d'un réseau de zombies qui utilise les ressources de votre ordinateur pour atteindre d'autres utilisateurs à leur insu.

- Référence

Good

bitwarden

Bureau fédéral d'enquête (FBI)

Évaluation globale du Bitwarden : Bonne

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
- Cite le besoin de 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

> "Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions."
>
> **FBI**

Commission fédérale du commerce (FTC)

Création de mots de passe forts et autres moyens de protéger vos comptes

Conseil de l'Agence :

- Une autre option consiste à utiliser un gestionnaire de mots de passe tiers pour créer un mot de passe fort - et s'en souvenir. Pour trouver un gestionnaire de mots de passe réputé, lisez les avis d'experts. Assurez-vous que le mot de passe que vous utilisez avec le gestionnaire de mots de passe est fort et sûr. Un navigateur web, un navigateur mobile et un gestionnaire de mots de passe peuvent tous sauvegarder vos mots de passe pour vous.
- Un mot de passe fort est une première étape importante dans la protection de votre compte contre les pirates informatiques. Mais même les mots de passe forts sont vulnérables aux cyberattaques. L'utilisation de l'authentification multifactorielle signifie qu'un pirate qui vole votre mot de passe ne peut pas se connecter à votre compte sans un autre facteur d'authentification.
- Le type d'authentification multifactorielle le plus courant est un code de vérification que vous recevez par SMS ou par courrier électronique. Ce code d'accès à usage unique est généralement composé de six chiffres ou plus et il expire automatiquement. Choisissez donc une méthode plus sûre, comme une application d'authentification ou une clé de sécurité, pour une meilleure protection, si vous en avez la possibilité.
- Référence

Liste de contrôle des mots de passe

Conseil de l'Agence :

- **Veillez à ce que votre mot de passe soit long et fort.** Cela signifie au moins 12 caractères. L'allongement du mot de passe est généralement le moyen le plus simple de le renforcer. Envisagez d'utiliser une phrase de passe composée de mots aléatoires afin que votre mot de passe soit plus mémorable, mais évitez d'utiliser des mots ou des phrases courants. Si le service que vous utilisez n'autorise pas les mots de passe longs, vous pouvez renforcer votre mot de passe en mélangeant des lettres majuscules et minuscules, des chiffres et des symboles.

- **Ne réutilisez pas les mots de passe que vous avez utilisés pour d'autres comptes.** Utilisez des mots de passe différents pour des comptes différents. Ainsi, si un pirate informatique obtient le mot de passe d'un compte, il ne pourra pas l'utiliser pour accéder à vos autres comptes.

- **Utilisez l'authentification multifactorielle lorsqu'elle est possible.** Certains comptes offrent une sécurité supplémentaire en exigeant quelque chose en plus du mot de passe pour se connecter à votre compte. C'est ce qu'on appelle l'authentification multifactorielle. Le "petit plus" dont vous avez besoin pour vous connecter à votre compte se divise en deux catégories :
  - Quelque chose que vous possédez - comme un code d'accès obtenu via une application d'authentification ou une clé de sécurité.
  - Quelque chose que vous êtes - comme un scan de votre empreinte digitale, de votre rétine ou de votre visage.

- **Envisagez un gestionnaire de mots de passe.** La plupart des gens ont du mal à garder une trace de tous leurs mots de passe. Plus un mot de passe est long et compliqué, plus il est fort, mais un mot de passe long peut aussi être plus difficile à retenir. Pensez à stocker vos mots de passe et vos questions de sécurité dans un gestionnaire de mots de passe réputé. Pour trouver un gestionnaire de mots de passe réputé, consultez des sites d'évaluation indépendants et demandez à vos amis et à votre famille de vous indiquer ceux qu'ils utilisent. Veillez à utiliser un mot de passe fort pour sécuriser les informations contenues dans votre gestionnaire de mots de passe.

- **Choisissez des questions de sécurité dont vous êtes le seul à connaître la réponse.** Si un site vous demande de répondre à des questions de sécurité, évitez de fournir des réponses qui sont disponibles dans les archives publiques ou faciles à trouver en ligne, comme votre code postal, votre lieu de naissance ou le nom de jeune fille de votre mère. N'utilisez pas de questions comportant un nombre limité de réponses que les attaquants peuvent facilement deviner, comme la couleur de votre première voiture. Vous pouvez même utiliser des réponses absurdes pour rendre les devinettes plus difficiles - mais si vous le faites, assurez-vous de pouvoir vous souvenir de ce que vous utilisez.

- **Modifiez rapidement vos mots de passe en cas de violation.** Si une entreprise vous informe qu'il y a eu une violation de données et qu'un pirate a pu obtenir votre mot de passe, changez immédiatement le mot de passe que vous utilisez avec cette entreprise et sur tout compte utilisant un mot de passe similaire.

- Référence

Excellent

bitwarden

Commission fédérale du commerce (FTC)

Évaluation globale du Bitwarden : Excellent

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité sont à jour et respectent les lignes directrices du NIST.
- présente les recommandations en matière de sécurité des mots de passe d'une manière claire, digeste et facile à trouver

"Use a password manager. A third-party password manager also can create a strong password. To find a reputable password manager, read expert reviews. Make sure the password for your password manager is strong. And protect it like you do your other passwords."

FTC

Département du commerce

Mois national de la cybersécurité : Se protéger en ligne

Conseil de l'Agence :

- Auparavant, la sagesse conventionnelle consistait à créer des mots de passe en utilisant des caractères spéciaux, des majuscules, des chiffres, des lettres et toute une série de règles arbitraires, y compris l'obligation de changer de mot de passe plusieurs fois par an. Les recherches montrent que chacun d'entre nous a réagi de la même manière : nous avons utilisé des mots de passe ou créé des variantes du même mot de passe parce qu'on nous avait demandé de mémoriser des dizaines de mots de passe uniques pour chaque site, chaque connexion ou chaque application.

- Nos instincts naturels ont créé une faiblesse dans notre sécurité en ligne et les cybercriminels en ont profité. La recherche sur l'utilisation des mots de passe a démontré la faiblesse inhérente au fait d'attendre des utilisateurs qu'ils mémorisent des mots de passe arbitrairement complexes, et l'importance de l'utilisation de l'authentification multifactorielle (AMF) pour protéger nos informations privées. Il est important de noter que notre réflexion sur ce sujet a évolué et que nous avons identifié les pratiques suivantes pour mieux nous protéger :
  - Lorsque vous devez utiliser un mot de passe, utilisez un mot de passe plus long (15 caractères ou plus) ou même des phrases de passe, car ils offrent une meilleure protection qu'un mot de passe plus court et arbitrairement complexe. Les phrases de passe présentent l'avantage supplémentaire d'être faciles à mémoriser.

  - L'utilisation de l'AFM (comme un code à usage unique envoyé par courriel ou une application d'authentification sur votre téléphone) ajoute une deuxième couche critique de protection contre un mot de passe compromis. L'AMF doit être mise en place dès qu'elle est disponible. Cela ne prend que quelques instants et vous permettra d'avoir l'esprit tranquille.

- Les gestionnaires de mots de passe, protégés par un mot de passe long et très fort, avec l'option MFA activée, nous permettent de créer des mots de passe uniques pour chaque site sans avoir à les mémoriser tous.

- Référence

Le NIST relève du ministère du commerce

Conseil de l'Agence :

- Assurer la sécurité de nos réseaux mondiaux interconnectés, ainsi que des appareils et des données connectés à ces réseaux, est l'un des défis majeurs de notre époque.

- Le ministère du commerce est chargé d'améliorer la sensibilisation et la protection en matière de cybersécurité, de protéger la vie privée, de maintenir la sécurité publique, de soutenir la sécurité économique et nationale et de permettre aux Américains de mieux gérer leur sécurité en ligne.
  - Le NIST publie la version 1.0 du cadre de protection de la vie privée
  - Le NIST propose un guide de démarrage rapide pour son catalogue de garanties en matière de sécurité et de protection de la vie privée
  - Le coin de la cybersécurité pour les petites entreprises

- Référence

Very Good

bitwarden

Département du commerce

Appréciation globale du Bitwarden : Très bon

- Recommande l'utilisation d'un gestionnaire de mots de passe
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité sont à jour et respectent les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Commission fédérale des communications (FCC)

Conseils aux petites entreprises en matière de cybersécurité

- Former les employés aux principes de sécurité. Établir des pratiques et des politiques de sécurité de base pour les employés, par exemple en exigeant des mots de passe robustes et en établissant des lignes directrices sur l'utilisation appropriée d'Internet, qui détaillent les sanctions en cas de violation des politiques de cybersécurité de l'entreprise. Établir des règles de comportement décrivant la manière de traiter et de protéger les informations sur les clients et autres données vitales.
- Exiger des employés qu'ils utilisent des mots de passe uniques et qu'ils les changent tous les trois mois. Envisagez la mise en œuvre d'une authentification multifactorielle qui exige des informations supplémentaires en plus du mot de passe pour accéder au site. Vérifiez auprès de vos fournisseurs qui traitent des données sensibles, en particulier les institutions financières, s'ils proposent une authentification multifactorielle pour votre compte.
- Référence

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Fair

bitwarden

Commission fédérale des communications (FCC)

Évaluation globale du Bitwarden : Passable

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
  - Liens vers des contenus axés sur la sécurité des mots de passe
  - Toutefois, le contenu est manifestement dépassé et pourrait être mieux organisé.
- ne mentionne pas systématiquement la nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
  - Le NIST recommande de modifier les mots de passe tous les trois mois.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Administration des petites entreprises (SBA)

Meilleures pratiques pour prévenir les cyberattaques

Conseil de l'Agence :

- Les employés et leurs communications professionnelles sont l'une des principales causes des violations de données dans les petites entreprises, car ils constituent des voies d'accès directes à vos systèmes. La formation des employés aux meilleures pratiques d'utilisation de l'internet peut contribuer grandement à la prévention des cyberattaques.
  - D'autres thèmes de formation seront abordés :
    - Repérer les courriels d'hameçonnage
    - Utiliser les bonnes pratiques de navigation sur Internet
    - Éviter les téléchargements suspects
    - Activation des outils d'authentification (par exemple, mots de passe forts, authentification multifactorielle, etc.)
    - Protéger les informations sensibles des fournisseurs et des clients
- Référence

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Good

bitwarden

Administration des petites entreprises (SBA)

Évaluation globale du Bitwarden : Bonne

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
- Cite le besoin de 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

Commission des valeurs mobilières et des changes (SEC)

En juillet 2023, la SEC "a adopté des règles finales qui exigeront des entreprises publiques qu'elles divulguent à la fois les incidents de cybersécurité importants qu'elles subissent et, sur une base annuelle, des informations importantes concernant leur gestion des risques de cybersécurité, leur stratégie et leur gouvernance". Étant donné le rôle de la SEC dans l'application de la conformité en matière de cybersécurité, il semble prudent d'évaluer ses propres conseils en matière de sécurité des mots de passe.

Une recherche sur la "sécurité des mots de passe" sur le site SEC.gov révèle 12 documents, qui semblent tous dater d'il y a plusieurs années. Une page est consacrée à la cybersécurité, mais elle propose des recommandations assez générales reprises de la CISA. Une alerte aux risques de cybersécurité de 2020 intitulée "Cybersecurity : Safeguarding Client Accounts against Credential Compromise" (Protéger les comptes clients contre la compromission des données d'identification) renvoie à un PDF qui traite du bourrage de données d'identification. Bien que le mot "mot de passe" soit utilisé tout au long du texte, la "sécurité du mot de passe" n'est pas explicitement mentionnée. Les "mots de passe forts" sont mentionnés dans le contexte ci-dessous :

Cybersécurité : Protéger les comptes clients contre la compromission des données d'identification

Conseil de l'Agence :

- Alors que les entreprises se préparent à faire face à des attaques de credential stuffing, le personnel de l'OCIE encourage les entreprises à examiner leurs pratiques actuelles (par exemple, MFA et autres pratiques décrites ci-dessus) et toute limitation potentielle de ces pratiques, et à se demander si les clients et le personnel de l'entreprise sont correctement informés sur la façon dont ils peuvent mieux sécuriser leurs comptes. Des clients informés La plupart des entreprises demandent à leurs clients et à leur personnel de créer et d'utiliser des mots de passe robustes. Toutefois, l'utilisation de mots de passe est moins efficace si les clients et/ou le personnel réutilisent les mots de passe d'autres sites. Pour plus d'efficacité, certaines entreprises ont informé et encouragé leurs clients et leur personnel à créer des mots de passe forts et uniques et à changer de mot de passe s'il y a des indications que leur mot de passe a été compromis.

The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

Fair

bitwarden

Commission des valeurs mobilières et des changes (SEC)

Évaluation globale du Bitwarden : Passable

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
- Appel à l'importance de mots de passe forts
  - Liens vers des contenus datés qui reconnaissent l'existence de mots de passe forts mais qui pourraient être beaucoup plus explicites
- Ne mentionne pas systématiquement la nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe.
  - Bien que le PDF mentionné ci-dessus fasse référence à l'AFC/ABF, il ne s'agit pas d'un conseil prolifique et il faut faire des recherches pour le trouver.
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver

La Maison Blanche

Proclamation sur le mois de la sensibilisation à la cybersécurité, 2023

Conseil de l'Agence :

- "J'appelle les citoyens, les entreprises et les institutions des États-Unis à reconnaître l'importance de la cybersécurité et à agir en conséquence, et à observer le mois de la sensibilisation à la cybersécurité pour soutenir notre sécurité et notre résilience nationales. J'invite également les entreprises et les institutions à prendre des mesures pour mieux protéger le peuple américain contre les cybermenaces et créer de nouvelles opportunités pour les travailleurs américains afin qu'ils puissent occuper des cyberemplois bien rémunérés. Les Américains peuvent également prendre des mesures immédiates pour mieux se protéger, notamment en activant l'authentification multifactorielle, en mettant à jour les logiciels sur les ordinateurs et les appareils, en utilisant des mots de passe forts et en restant prudents lorsqu'ils cliquent sur des liens qui leur paraissent suspects.
- Référence

Offrir au public une expérience numérique de premier plan

Conseil de l'Agence :

- Les agences veillent à ce que les sites web qui demandent au public de s'authentifier soient compatibles avec les gestionnaires de mots de passe couramment utilisés et n'empêchent pas le "collage" de mots de passe ou d'autres mécanismes d'assistance automatisés côté client.
- Référence

Compte rendu du symposium de la Maison Blanche sur la modernisation de l'authentification multifactorielle

Conseil de l'Agence :

- "Il faut plus qu'un mot de passe pour rester en sécurité en ligne – et c'est là que l'authentification multifactorielle intervient pour garantir que vos données sont mieux protégées contre les cyberacteurs malveillants", a déclaré Brandon Wales, directeur exécutif de la CISA. "La CISA n'a cessé d'exhorter les organisations à mettre en œuvre l'AMF pour tous les utilisateurs afin de s'assurer que toutes les données critiques sont plus difficiles d'accès. Le symposium d'aujourd'hui a pour but de se réunir pour définir la vision que nous nous efforçons tous de concrétiser".

- Référence

L'administration Biden-Harris annonce un programme d'étiquetage de la cybersécurité pour les appareils intelligents afin de protéger les consommateurs américains

Conseil de l'Agence

- Agissant dans le cadre de son autorité de régulation des dispositifs de communication sans fil, la FCC devrait solliciter les commentaires du public sur le déploiement du programme volontaire d'étiquetage de la cybersécurité proposé, qui devrait être opérationnel en 2024. Tel que proposé, le programme s'appuierait sur les efforts des parties prenantes pour certifier et étiqueter les produits, sur la base de critères de cybersécurité spécifiques publiés par le National Institute of Standards and Technology (NIST) qui, par exemple, exige des mots de passe par défaut uniques et forts, la protection des données, des mises à jour logicielles et des capacités de détection d'incidents.

- Référence

Good

Updated January 2025

bitwarden

La Maison Blanche

Évaluation globale du Bitwarden : Bonne

- Ne recommande pas l'utilisation d'un gestionnaire de mot de passe
  - Dans une communication publiée en 2022 dans le cadre du mois de la sensibilisation à la cybersécurité, la Maison Blanche a recommandé l'utilisation d'un gestionnaire de mots de passe. La Maison Blanche a eu l'occasion de faire de même avec le blog 2023 Cybersecurity Awareness. Ce n'est pas le cas. Bien que le blog recommande "l'utilisation de mots de passe forts", il ne mentionne pas les gestionnaires de mots de passe.
- Appel à l'importance de mots de passe forts
- La nécessité de mettre en place un système 2FA/MFA pour renforcer la sécurité des mots de passe
- Les conseils généraux en matière de sécurité ne sont pas actualisés et ne respectent pas les lignes directrices du NIST.
  - Dans des communications antérieures, la Maison Blanche a recommandé de changer les mots de passe, en contradiction avec les conseils du NIST. Les mots de passe ne doivent être modifiés que s'ils sont faibles, réutilisés ou compromis. Un mot de passe fort et unique n'a jamais besoin d'être modifié, sauf si vous soupçonnez qu'il a été compromis.
- ne présente pas les recommandations en matière de sécurité des mots de passe de manière claire, digeste et facile à trouver
  - Pas de page dédiée à la cybersécurité

Récapitulatif

Vous pouvez prendre de nombreuses mesures pour assurer votre sécurité en ligne, mais l'action la plus simple ayant l'impact le plus important et le plus immédiat sur votre sécurité est l'utilisation d'un gestionnaire de mots de passe. Choisissez un gestionnaire de mots de passe multiplateforme doté d'un système de cryptage de bout en bout sans connaissance, capable de générer et de stocker un nombre illimité de mots de passe uniques et robustes. Vous pouvez commencer à utiliser Bitwarden avec un compte gratuit ou opter pour un compte Premium pour moins de 10 $/an afin d'obtenir des fonctionnalités avancées.

Ressources complémentaires

- Voir la présentation sur l'état de la sécurité des mots de passe