Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice sur la sécurité des mots de passe

Publié : le 2025-10-20

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT48-58/2025F-PDF
ISBN: 978-0-660-79023-7

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guideline on Password Security

Ligne directrice sur la sécurité des mots de passe

Sur cette page

1. Introduction

▶ Dans cette section

1.1 Contexte

Alors que le gouvernement du Canada (GC) compte de plus en plus sur les technologies numériques, il doit continuer de renforcer ses défenses contre l'accès non autorisé aux données sensibles et aux systèmes de technologie de l'information (TI). Les mots de passe faibles et compromis sont l'une des principales causes d'atteintes à la sécurité, et même les mots de passe forts peuvent être sapés par des tactiques telles que l'enregistrement de frappe et le piratage psychologique.

Les recherches sur les mots de passe piratés ont donné lieu à des informations précieuses sur les mots de passe créés par les personnes et ont permis de mettre en place de nouvelles pratiques exemplaires en matière d'authentification basée sur un « élément connu » ou sur des mots de passe. Par le passé, les mots de passe ont été la principale forme d'authentification, mais ils ne devraient plus être le seul mécanisme utilisé. Les personnes ont souvent été contraintes de créer des mots de passe complexes, ce qui a conduit à des pratiques peu sures. Les comptes mal sécurisés présentent des vulnérabilités importantes, offrant aux pirates informatiques des points d'ancrage éventuels pour compromettre des systèmes entiers par des méthodes telles que l'hameçonnage ou le piratage psychologique. Si l'adoption de bonnes pratiques en matière de mots de passe est essentielle, il reste qu'elle ne constitue qu'un élément d'une stratégie globale de sécurité des TI. Pour protéger efficacement ses biens, le GC a besoin d'une approche qui assure des mesures d'authentification robustes, tout en allégeant le fardeau qui pèse sur les personnes qui utilisent les systèmes.

1.2 Objet et champ d'application

Les présentes lignes directrices ont pour but :

- de mettre en place des pratiques exemplaires pour assurer une gestion sécurisée des mots de passe au sein du GC;
- de fournir des conseils et une orientation que les propriétaires de systèmes au GC peuvent prendre en considération au moment de mettre en œuvre un système d'authentification basée sur des mots de passe, peu importe s'il est utilisé comme seule méthode d'authentification (ce qui n'est pas recommandé) ou avec une solution multifactorielle.

Le champ d'application des présentes lignes directrices s'étend aux mots de passe qui sont utilisés par des personnes et ne couvre pas les entités non humaines, par exemple les comptes de service, qui ne sont pas limitées par la mémoire ou le comportement humain. Pour les comptes gérés numériquement, il faudrait utiliser des systèmes automatisés pour assurer une modification fréquente des mots de passe longs et complexes, au besoin.

1.3 Public visé

Le présent document s'adresse principalement aux propriétaires de systèmes du GC et contient des lignes directrices à l'intention du personnel du GC qui utilise ces systèmes.

2. Aider les personnes qui utilisent les systèmes à vous aider

▶ Dans cette section

2.1 Favoriser la longueur plutôt que la complexité

Par le passé, les personnes devaient créer des mots de passe complexes comprenant des lettres minuscules et majuscules, un chiffre et des caractères spéciaux pour assurer la mise en place de mots de passe plus forts. En fait, cette approche a eu l'effet contraire. Puisqu'elles ont du mal à se souvenir d'un nombre croissant de mots de passe complexes et arrivant à expiration, les personnes qui utilisent les systèmes font souvent le strict minimum pour répondre aux exigences de complexité du GC. Par exemple, l'un des mots de passe les plus courants est « mot de passe ». Pour répondre aux exigences de complexité, un nombre alarmant de personnes utilisent « Motdepasse1 » ou « Motdepasse2! ».

Pour faciliter la tâche des personnes lorsqu'elles doivent créer de meilleurs mots de passe, les propriétaires de systèmes du GC devraient prendre les mesures suivantes :

- abolir ou assouplir les politiques sur la complexité (par exemple, autoriser les mots de passe composés de lettres minuscules auxquels les personnes concernées peuvent, si elles le souhaitent, ajouter des lettres majuscules et d'autres caractères);
- exiger un nombre minimal de caractères (au moins 12) et inviter les personnes concernées à créer des mots de passe aussi longs qu'elles le souhaitent, dans les limites du raisonnable (par exemple, 64 caractères ou moins) [1];
- autoriser les phrases de passe composées d'au moins quatre ou cinq mots choisis au hasard pour satisfaire à l'exigence de longueur minimale de 12 caractères;
- dans les environnements Windows, envisager la possibilité de créer des mots de passe comportant au moins 15 caractères [2] afin d'éviter de stocker de mots de passe faibles pour les gestionnaires de réseau local (LAN).

Se reporter à l’annexe B pour connaître la longueur minimale recommandée du mot de passe lorsqu’il est nécessaire de créer des mots de passe comportant un certain degré de complexité (par exemple, dans les systèmes existants ou en raison de limitations technologiques).

2.2 Éliminer les dates d’expiration des mots de passe

L’obligation de changer les mots de passe régulièrement représente un fardeau important pour les personnes concernées et a peu d’effet sur la sécurité. Les périodes habituelles de validité des mots de passe contribuent peu à éviter le craquage de ceux-ci, car dès qu’un mot de passe est craqué, les pirates informatiques ont amplement le temps d’exploiter le système. De plus, les personnes ont tendance à choisir des mots de passe peu sûrs qui sont tous semblables et prévisibles.

Par conséquent, les propriétaires de systèmes du GC devraient exiger des personnes concernées qu’elles changent leurs mots de passe seulement lorsqu’il y a une bonne raison de le faire, par exemple, en cas d’atteinte avérée ou soupçonnée ou de modification des exigences liées aux mots de passe en raison d’une nouvelle politique. Avant d’imposer des changements de mot de passe, les propriétaires de systèmes doivent réfléchir aux répercussions que cela aura sur les utilisateurs. Si un compte est sécurisé et répond à toutes les exigences de la politique, on ne doit pas demander à son utilisateur de changer de mot de passe inutilement. De même, si la sécurité est compromise, les utilisateurs ne doivent pas réutiliser leurs anciens mots de passe.

2.3 Dresser une liste noire de certains mots de passe

Les analyses d’intrusions passées ont révélé qu’un nombre ahurissant de personnes utilisent des mots de passe, comme « motdepasse » ou « 123456 ». L’élaboration d’une liste noire (ou de blocage) des mots de passe

qui sont répandus ou faciles à deviner, dont ceux qui font référence au Canada, qui contiennent le nom d'une équipe de hockey locale ou qui figurent dans des listes de mots de passe ayant donné lieu à une atteinte à la sécurité d'un système, peut réduire la probabilité d'une attaque par dictionnaire réussie.

Les propriétaires de systèmes du GC qui emploient la liste noire des mots de passe devraient s'assurer que les systèmes indiquent aux personnes concernées la raison pour laquelle un mot de passe en particulier est refusé lorsqu'elles tentent d'utiliser un mot de passe figurant sur la liste noire.

2.4 Fournir un gestionnaire de mot de passe

Les gestionnaires de mots de passe sont des applications qui, au minimum, servent à stocker les mots de passe en toute sécurité. Ces applications peuvent aussi être utilisées, par exemple, pour :

- générer des mots de passe forts et aléatoires;
- automatiser l'authentification en interagissant directement avec les invites d'ouverture de session;
- faciliter le remplissage des champs habituels des formulaires, comme le nom et l'adresse.

De plus, les gestionnaires de mots de passe sont un excellent outil pour aider les personnes qui utilisent les systèmes à composer avec la surabondance de mots de passe. Ils favorisent aussi l'utilisation de mots de passe forts et complexes et découragent la réutilisation des mots de passe.

Bien que les gestionnaires de mots de passe offrent de nombreux avantages, ils comportent aussi de nombreux risques. Le plus grand risque découle du fait que, s'ils sont compromis, tous les comptes associés aux

mots de passe qui y sont stockés peuvent l'être également. Dans une certaine mesure, le gestionnaire de mots de passe détient les « clés du royaume » d'une personne qui utilise un système.

Se reporter à l'annexe D pour obtenir d'autres informations.

2.5 Éviter d'utiliser des comptes partagés ou, le cas échéant, en gérer l'utilisation

Les comptes partagés sont fortement déconseillés en raison des risques importants et des défis opérationnels qu'ils posent. Le principal problème est l'absence de responsabilisation, car lorsqu'un groupe partage les mêmes identifiants, il devient difficile de déterminer qui a effectué l'activité particulière. Il est alors aussi difficile d'enquêter sur les incidents de sécurité, car les journaux d'audit peuvent ne pas indiquer clairement la personne responsable d'une activité en particulier.

Si l'utilisation de comptes partagés est inévitable et qu'elle peut être justifiée sur le plan opérationnel, il convient de mettre en œuvre des mesures de sécurité strictes pour atténuer les risques connexes. Par exemple, les mots de passe doivent être renouvelés régulièrement ou immédiatement chaque fois qu'une personne quitte le groupe. Ainsi, il sera possible de s'assurer que les membres du groupe qui avaient par le passé accès au système n'y ont plus accès, et de réduire le risque d'accès non autorisé.

La fréquence du renouvellement des mots de passe doit être déterminée par certains facteurs, notamment les suivants :

- la sensibilité du bien auquel le groupe aura accès;
- la probabilité que des membres qui ne font plus partie du groupe tentent d'accéder à l'interface d'authentification;
- le taux de roulement des membres du groupe.

Comme mesure d'atténuation supplémentaire, il est possible d'utiliser un coffre-fort de sécurité ou un gestionnaire de mots de passe qui peut suivre et auditer l'accès aux mots de passe après leur utilisation.

3. Mettre en œuvre des mesures pour contrer les attaques en ligne

▶ Dans cette section

Les attaques sur les mots de passe se produisent lorsque des pirates informatiques interagissent avec l'écran d'ouverture de session d'un système et saisissent des mots de passe devinés pour un ou plusieurs comptes. Il peut s'agir d'attaques automatisées provenant de plusieurs sources distribuées (par exemple, réseau d'ordinateurs zombies).

Parmi les mesures de défense contre les attaques par tentative de deviner un mot de passe en ligne figurent les suivantes :

- le ralentissement artificiel;
- le verrouillage;
- la surveillance et l'authentification fondée sur les risques;
- l'authentification multifactorielle;
- les procédures de réinitialisation sécurisée des mots de passe.

3.1 Le ralentissement artificiel

Le ralentissement artificiel permet de restreindre le nombre de tentatives autorisées pour ouvrir une session dans un compte en particulier au cours d'une période donnée. Dans son Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information – ITSP.30.031, le Centre de la sécurité des télécommunications Canada recommande un maximum de 100 tentatives dans une période de 30 jours.

Lorsqu'il est utilisé avec une liste noire des mots de passe, le ralentissement artificiel peut nuire considérablement à l'efficacité des attaques de mot de passe en ligne.

3.2 Le verrouillage

Le verrouillage bloque l'accès à un compte après un nombre préétabli de tentatives de mots de passe incorrectes. Par exemple, un système pourrait verrouiller un compte après 10 tentatives infructueuses.

Il faut établir un juste équilibre entre la nécessité de prévenir une attaque par tentative de deviner en ligne et la nécessité de tenir compte du fait que les personnes qui utilisent en toute légitimité les systèmes taperont, de temps à autre, leur mot de passe incorrectement.

3.3 La surveillance et l'authentification fondée sur les risques

La surveillance des tentatives d'ouverture de session (par exemple, en fonction de l'adresse IP et de l'heure de la journée) dans le but de détecter toute activité anormale est une autre façon de prévenir les attaques par tentative de deviner le mot de passe en ligne.

Les mécanismes de surveillance devraient pouvoir détecter toute activité anormale suivante :

- un grand nombre de tentatives infructueuses d'ouvertures de session dans un compte individuel;
- un grand nombre de tentatives infructueuses d'ouvertures de session dans de nombreux comptes.

L’authentification fondée sur le risque peut permettre d’obtenir une réponse adaptable à la mesure de surveillance utilisée en calculant la cote de risque, puis en appliquant les mesures de contrôle en matière d’authentification en fonction de la cote obtenue. L’authentification fondée sur le risque permettrait ainsi d’analyser une tentative d’authentification à partir d’une adresse IP inhabituelle ou à un moment inhabituel, ou une tentative effectuée à la fois à partir d’une adresse IP inhabituelle et à un moment inhabituel, puis d’appliquer les mesures de contrôle supplémentaires, comme poser une question de sécurité ou simplement refuser l’accès.

3.4 L’authentification multifactorielle

L’authentification multifactorielle (AMF) renforce la sécurité des comptes en prévoyant au moins deux étapes pendant le processus d’ouverture de session.

À mesure que la puissance de calcul augmente et que les outils conçus pour mener les attaques s’améliorent (par exemple, logiciels de craquage de mots de passe basés sur l’intelligence artificielle), il sera essentiel d’utiliser l’AMF pour assurer un niveau de sécurité élevé. Sans AMF, les mots de passe devront être de plus en plus longs, ce qui alourdira le fardeau des personnes qui utilisent les systèmes. Par conséquent, il est fortement recommandé de mettre en œuvre l’AMF pour toutes les personnes concernées dans tous les processus d’authentification au sein du GC afin de réduire le risque de piratage de compte et de renforcer la sécurité globale du GC.

Pour obtenir d’autres informations, se reporter à la Ligne directrice du gouvernement du Canada (GC) sur l’authentification multifactorielle (AMF) : Recommandations techniques relatives aux authentifiants utilisés pour l’AMF dans le domaine opérationnel du GC.

3.5 Les procédures de réinitialisation sécurisée des mots de passe

Il faut absolument mettre en place une procédure de réinitialisation sécurisée des mots de passe pour protéger les comptes et empêcher tout accès non autorisé à ceux-ci. Tout processus de récupération de mot de passe, notamment la réinitialisation de mot de passe en libre-service, doit être au moins aussi sécurisé que la ou les méthodes utilisées pour créer le compte si le mot de passe est le seul authentifiant utilisé.

Les paragraphes suivants décrivent les éléments à prendre en considération pour réinitialiser des mots de passe au moyen de liens transmis par courriel par opposition aux procédures visant des questions de sécurité.

- Liens de réinitialisation transmis par courriel
    - Les liens de réinitialisation doivent être envoyés uniquement à une adresse électronique préenregistrée, vérifiée et qui est contrôlée par le GC.
    - Les liens doivent être temporaires et, donc, expirer après une certaine période pour limiter la fenêtre d'utilisation abusive possible (5 à 10 minutes).
    - Les jetons générés doivent être uniques, aléatoires et valides pour une seule utilisation. Un jeton doit être stocké en toute sécurité et lié au compte.
- Questions de sécurité
    - Aussi connues sous le nom d'authentification basée sur la connaissance, les questions de sécurité ne sont plus considérées comme une méthode d'authentification acceptable et ne devraient plus être utilisées. Les pirates informatiques peuvent découvrir les réponses à de nombreuses questions pour lesquelles il y a un nombre limité de choix de réponse possibles, ce qui entraîne un

risque inacceptable d’exploitation réussie par des personnes non autorisées.

4. Mettre en œuvre des mesures pour contrer les attaques hors ligne

▶ Dans cette section

Une attaque hors ligne survient lorsque des pirates informatiques obtiennent la base de données des mots de passe d’un système et lancent une attaque contre les mots de passe stockés.

Une telle attaque permet de contourner les contre-mesures d’attaque en ligne susmentionnées et donne aux pirates une puissance de calcul accrue qui leur permet, par exemple, de faire des milliards de tentatives par seconde pour deviner des mots de passe. Par conséquent, elle peut dévoiler rapidement de nombreux mots de passe de systèmes si les propriétaires n’ont pas mis en place certaines contre-mesures.

Les mesures de protection contre les attaques hors ligne comprennent :

- le hachage;
- le salage;
- le hachage à clé.

La longueur du mot de passe est particulièrement importante pour assurer une bonne protection contre les attaques hors ligne.

4.1 Le hachage

Le « hachage » est un moyen de transformer des informations, telles qu’un mot de passe, en un mélange de caractères brouillés qui ne peuvent pas être reconstitués. Les mots de passe ne doivent jamais être stockés sous

forme de texte brut. Les systèmes doivent hacher les mots de passe à l'aide d'algorithmes de hachage modernes et approuvés décrits dans les Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B : ITSP.40.111 du Centre canadien pour la cybersécurité (par exemple, fonction de dérivation de clés fondée sur un mot de passe 2 [PBKDF2 pour *Password-Based Key Derivation Function* 2]).

Le hachage est un processus à sens unique, ce qui signifie qu'il ne peut pas être inversé pour récupérer le mot de passe d'origine. Cette caractéristique le rend idéal pour la validation des mots de passe, car même si des pirates informatiques obtiennent le mot de passe haché, celui-ci ne pourra pas être utilisé pour ouvrir une session du système.

Cependant, les pirates informatiques peuvent tenter de craquer ou de désosser les mots de passe en :

- utilisant des listes obtenues à partir de failles de sécurité précédentes;
- utilisant des listes de mots provenant de dictionnaires;
- essayant des attaques par force brute.

Bien que le nombre de permutations puisse être énorme, le faible coût du matériel à haut débit, la tendance des personnes à choisir des mots de passe communs et l'informatique en nuage rendent le craquage de mots de passe de plus en plus réalisable.

Pour contrer ce risque, les systèmes devraient permettre de mettre en œuvre l'itération de hachage afin d'augmenter le coût de calcul par tentative de deviner pour les pirates informatiques. Un minimum de 10 000 itérations est recommandé.

4.2 Le salage

Le « salage » rend un mot de passe plus sûr en y ajoutant des informations aléatoires supplémentaires avant de le hacher. Les données supplémentaires sont différentes pour chaque personne et permettent d'empêcher les pirates d'utiliser des listes prédéfinies (appelées tables arc-en-ciel) pour craquer les mots de passe. Comme chaque sel est unique à chaque personne (par exemple, en étant basé sur ses identifiants) et qu'il est généré de manière aléatoire, il est nettement plus difficile de craquer un grand nombre de hachages, car le temps nécessaire augmente directement avec le nombre de hachages. Si le salage n'est pas possible, il est encore plus important d'utiliser d'autres contre-mesures pour protéger les mots de passe.

4.3 Le hachage à clé

Une autre mesure de protection du stockage des mots de passe consiste à combiner le mot de passe à une clé secrète avant de procéder au hachage. Il est possible d'utiliser une valeur secrète (parfois appelée « poivre ») pour toutes les personnes qui utilisent le système, en plus du salage, afin d'ajouter une autre couche de sécurité, ce qui complique davantage la tâche des pirates informatiques lors d'une tentative de craquage des hachages en cas d'intrusion dans une base de données. Contrairement aux sels, qui sont stockés dans la base de données avec les mots de passe hachés, la valeur secrète est conservée dans un emplacement sécurisé, par exemple dans l'application elle-même ou, idéalement, dans un coffre-fort secret ou un module de sécurité matériel.

Dans le cas d'une intrusion dans une base de données, les pirates informatiques peuvent avoir accès aux sels et aux hachages, mais pas au poivre. Cette couche de protection supplémentaire augmente considérablement la difficulté de désosser les hachages, car les pirates

informatiques auraient besoin de deviner ou de découvrir le poivre. Par conséquent, cette approche renforce la sécurité contre les attaques hors ligne.

Le hachage à clé est une technique qui consiste à hacher les mots de passe à l'aide d'une clé cryptographique qui peut être propre à chaque personne ou groupe de personnes qui utilise le système.

Bien que cette mesure ne soit pas disponible pour tous les systèmes, elle offre le plus haut niveau de protection des mots de passe qui soit disponible dans la pratique.

5. Références

1. Centre de la sécurité des télécommunications Canada, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3), avril 2018
2. Royaume-Uni, National Cyber Security Centre, Password administration for system owners, novembre 2018
3. États-Unis, National Institute of Standards and Technology Special Publication 800-63-3, Digital Identity Guidelines: Authentication and Lifecycle Management, juin 2017.
4. Gouvernement de l'Australie, Australian Cyber Security Centre, Passphrases, novembre 2017.
5. Robyn Hicock, Microsoft Identity Protection Team, Microsoft Password Guidance.
6. J. Bonneau, C. Herley, P.C. van Oorschot et F. Stajano. Passwords and the Evolution of Imperfect Authentication. Communications of the Association for Computing Machinery (ACM), vol. 58, nº 7, juillet 2015), pages 78 à 87.

7. D. Florêncio, C. Herley et P.C. van Oorschot. An Administrator’s Guide to Internet Password Research, USENIX LISA, novembre 2014.
8. Open Worldwide Application Security Project, Password Storage Cheat Sheet. [Accédé le 19 novembre 2024.]

6. Demandes de renseignements

Pour obtenir des renseignements supplémentaires ou des précisions concernant les présentes lignes directrices, veuillez faire parvenir un courriel à l’adresse ZZTBSCYBERS@tbs-sct.gc.ca.

Annexe A. Glossaire

réseau de zombies
Ensemble d’ordinateurs ou d’appareils compromis (« zombies ») qui exécutent des applications malveillantes à l’insu de la personne concernée au moyen d’une infrastructure de commande et de contrôle.

hachage
Fonction qui fait correspondre une chaîne de bits de longueur aléatoire à une chaîne de bits de longueur fixe.

hameçonnage
Tentative effectuée par une tierce partie qui vise à obtenir des renseignements confidentiels auprès d’une personne, d’un groupe ou d’une organisation en imitant une marque particulière, généralement bien connue, ou en usurpant leur identité, habituellement à des fins financières. Les pirates essaient d’amener les destinataires à leur communiquer des données personnelles, comme des numéros de carte de crédit ou des justificatifs bancaires en ligne pour ensuite les utiliser pour commettre des actes frauduleux.

hachage à clé

Type de hachage qui implique une clé secrète dans le calcul de la valeur de hachage. Contrairement au hachage standard, qui est déterministe et public, le hachage à clé (par exemple, code d'authentification de message fondé sur le hachage [HMAC]) garantit à la fois l'intégrité et l'authenticité. Il vérifie qu'un message n'a pas été modifié et qu'il provient d'une source fiable.

table arc-en-ciel
Table précalculée permettant d'inverser les fonctions de hachage cryptographiques, généralement utilisée pour craquer les hachages de mot de passe.

salage
Valeur non secrète utilisée dans un processus cryptographique, habituellement pour s'assurer que les résultats des calculs effectués pour un cas ne peuvent pas être réutilisés par des pirates informatiques.

hameçonnage ciblé
Technique qui consiste à utiliser des courriels frauduleux ayant pour but de persuader les membres du personnel d'une organisation de révéler leurs identifiants ou leur mot de passe. Contrairement à l'hameçonnage, qui consiste en un envoi massif de messages courriel, l'hameçonnage ciblé se fait à petite échelle et de manière ciblée.

Annexe B. Équivalence de la complexité des mots de passe

Bien que l'approche privilégiée consiste à éliminer les exigences de complexité des mots de passe au profit de l'application d'une longueur minimale de mot de passe de 12 caractères, ce n'est pas toujours possible de le faire, en particulier dans les systèmes existants ou lorsqu'il existe des contraintes techniques. Dans de tels cas, l'augmentation de la complexité

des mots de passe peut contribuer à améliorer l'entropie, une mesure du degré d'imprévisibilité et de résistance d'un mot de passe aux attaques par tentative de deviner le mot de passe ou par force brute.

L'entropie augmente lorsque les mots de passe comprennent un ensemble diversifié de caractères, tels que des lettres majuscules et minuscules, des chiffres et des symboles spéciaux. Cependant, la complexité seule n'est pas suffisante si le mot de passe suit des modèles courants ou prévisibles. Par exemple, le mot de passe « Motdepasse123! » semble complexe, mais il est facile à deviner et offre une faible entropie effective.

Pour assurer une sécurité renforcée des mots de passe, en particulier ceux de moins de 12 caractères, il est fortement recommandé de les générer de manière aléatoire, idéalement à l'aide d'un gestionnaire de mots de passe réputé capable de créer des mots de passe à haute entropie, à la fois complexes et difficiles à deviner.

Le tableau B1 indique la longueur minimale recommandée du mot de passe lorsqu'il est nécessaire d'assurer un certain degré de complexité du mot de passe.

Tableau B1. Longueur minimale du mot de passe recommandée pour différents degrés de complexité

Degré de complexité	Longueur minimale du mot de passe
Présence de lettres majuscules et minuscules	10 caractères
Présence de caractères alphanumériques	9 caractères
Présence de caractères alphanumériques et de caractères spéciaux	8 caractères

Annexe C. Orientation sur les mots de passe pour le personnel du gouvernement du Canada

▼ Dans cette section

La longueur et la complexité du mot de passe

Il est plus efficace d'utiliser des mots de passe plus longs et plus simples que des mots de passe plus courts et plus complexes.

Par « complexité du mot de passe », on entend une combinaison de caractères dans un mot de passe. Un mot de passe qui ne contient que des lettres minuscules n'est pas complexe, mais un mot de passe qui contient des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux est complexe.

À première vue, il peut sembler que le fait d'obliger les personnes à recourir à des mots de passe complexes donne lieu à des mots de passe plus forts. Toutefois, puisqu'ils sont complexes, ces mots de passe sont plus difficiles à retenir, de sorte que les personnes réutilisent souvent les mêmes mots de passe, ce qui réduit ultimement la sécurité d'ensemble.

En outre, l'analyse des mots de passe utilisés lors d'intrusions antérieures montre que les personnes choisissent des modèles prévisibles lorsqu'elles doivent rendre un mot de passe plus complexe. Par exemple, elles mettent

la première lettre en majuscule et utilisent un point d’exclamation comme dernier caractère.

Les mots de passe plus longs, mais moins complexes, comme ceux qui comportent quatre ou cinq mots choisis aléatoirement, sont ainsi plus forts. Le fait qu’ils soient plus longs permet de compenser le fait qu’ils soient moins complexes. De plus, le fait d’en réduire le degré de complexité permet aux personnes concernées de créer des mots de passe plus faciles à retenir.

Lorsqu’un mot de passe simple en minuscules est utilisé, il doit comporter au moins 12 lettres.

Réutilisation des mots de passe

Les intrusions passées dans les systèmes ont donné aux pirates informatiques l’accès à plus de 3 milliards de mots de passe. Ces mots de passe compromis sont un bon point de départ pour les attaques par tentative de deviner des mots de passe. Les personnes qui utilisent les systèmes devraient donc éviter de réutiliser leurs mots de passe. Un mot de passe compromis qui est obtenu à la suite d’une intrusion dans un système peut ouvrir la voie aux intrusions dans d’autres systèmes.

Idéalement, les mots de passe devraient être uniques à chaque système. Au minimum, les personnes concernées ne devraient pas utiliser les mêmes mots de passe pour leurs comptes personnels et pour leurs comptes du GC. Elles devraient également envisager d’utiliser des mots de passe uniques pour les comptes les plus importants, en particulier ceux qui servent à récupérer des mots de passe.

Authentification multifactorielle

De nombreux systèmes offrent maintenant aux personnes concernées la possibilité d'utiliser une AMF en leur envoyant, par exemple, un code à usage unique ou une invite par message texte ou au moyen d'une application. L'utilisation de l'AMF peut empêcher que des comptes soient compromis. Les personnes concernées devraient donc utiliser l'AMF, particulièrement si elles utilisent des réseaux non fiables comme Internet. Elles devraient également envisager d'utiliser l'AMF pour leurs comptes personnels, comme Google, Apple, Facebook, LinkedIn et Twitter, afin d'éviter que ceux-ci soient utilisés pour lancer des attaques d'hameçonnage ciblé contre les comptes du GC.

Conseils pour les mots de passe

Les conseils ci-dessous peuvent aider les personnes concernées à créer et à gérer des mots de passe sécurisés.

- Utiliser une phrase de passe. Les phrases de passe sont plus faciles à retenir et peuvent être aussi sures que les mots de passe plus courts et plus complexes.
    - choisir quatre ou cinq mots au hasard (par exemple, « bon cheval agrafe batterie »);
    - insérer certains mots d'une autre langue (par exemple, « bon horse agrafe batterie »);
    - essayer d'appliquer le procédé de Schneier (en anglais seulement) (par exemple, « J'aime manger de la pizza tous les jeudis pour souper » devient quelque chose comme « Jmdlptljps »);
    - ne pas utiliser, notamment, d'expressions courantes, de titres ou de paroles de chansons, de titres de films ou de citations.
- Soumettre le mot de passe éventuel à un « test de 20 tentatives pour le deviner », afin de vérifier si une personne qui connaît bien la personne

concernée ou qui a accès au contenu des médias sociaux de cette dernière peut deviner son mot de passe en 20 tentatives. Ne pas inclure de renseignements personnels dans les mots de passe, par exemple une date de naissance ou de mariage, ou le nom de membres de la famille), car ce type de renseignements peut être facile à deviner.

- Rendre le mot de passe plus complexe, sans qu'il soit trop difficile à retenir. En général, chaque caractère ou chaque mot supplémentaire renforce le mot de passe ou la phrase de passe.
- Utiliser un gestionnaire de mots de passe pour générer un mot de passe fort (voir l'annexe D pour obtenir des conseils sur les gestionnaires de mots de passe).
- Ne pas utiliser des techniques prévisibles comme le remplacement de « E » par « 3 » ou de « a » par « @ ». De telles techniques donnent un faux sentiment de sécurité et rendent le mot de passe très vulnérable aux attaques par tentative de deviner automatisées.
- S'il faut un mot de passe complexe, ne pas se contenter de mettre la première lettre en majuscule et de terminer le mot de passe par un signe de ponctuation (surtout par un point d'exclamation) (par exemple, « motdepasse » devient « Motdepasse! »). De tels mots de passe sont faciles à deviner.
- Éviter d'utiliser le nom d'une saison combiné à l'année pour composer un mot de passe (par exemple, « Été2018 »). Il s'agit d'une stratégie de composition de mots de passe répandue, de sorte que ces mots de passe sont faciles à deviner.
- Ne pas stocker les mots de passe en texte brut ou dans un format non chiffré (par exemple, dans un document texte ou dans une application permettant la prise de notes).
- Ne pas utiliser l'un ou l'autre des exemples de mot de passe susmentionnés.

Annexe D. Orientation sur les gestionnaires de mots de passe pour le personnel du gouvernement du Canada

Les gestionnaires de mots de passe sont des applications qui, au minimum, servent à stocker les mots de passe en toute sécurité. Ils peuvent aussi, par exemple :

- générer des mots de passe forts et aléatoires;
- automatiser l'authentification en interagissant directement avec les invites d'ouverture de session;
- faciliter le remplissage des champs habituels, comme le nom et l'adresse, des formulaires.

De plus, les gestionnaires de mots de passe sont un excellent outil pour aider les personnes concernées à composer avec la surabondance de mots de passe. Ils favorisent aussi l'utilisation de mots de passe forts et complexes, et ils découragent la réutilisation des mots de passe.

Bien que les gestionnaires de mots de passe offrent de nombreux avantages, ils comportent aussi de nombreux risques. Le plus grand risque découle du fait que, s'ils sont compromis, tous les comptes associés aux mots de passe qui y sont stockés peuvent l'être également. Dans une certaine mesure, le gestionnaire de mot de passe détient les « clés du royaume » d'une personne qui utilise un système.

Conseils sur l'utilisation des gestionnaires de mots de passe

- Ne pas stocker les mots de passe du GC sur vos appareils personnels.
- Utiliser uniquement les gestionnaires de mots de passe offerts par les prestataires jouissant d'une bonne réputation.
- Utiliser, dans la mesure du possible, un gestionnaire de mots de passe assorti d'une capacité d'AMF.

- Éviter d’y inscrire les mots de passe les plus importants.
- Ne pas y stocker de comptes privilégiés.
- Choisir un mot de passe illimité pour le gestionnaire de mots de passe qui est aussi sûr, voire davantage, que le mot de passe le plus fort qui y est stocké.
- Faire preuve de vigilance lorsqu’il s’agit d’installer les mises à jour du gestionnaire de mots de passe.

Des conseils supplémentaires sont disponibles sur le site GCéchange de la collectivité de cybersécurité du GC (en anglais seulement et accessible uniquement sur le réseau du gouvernement du Canada).

Notes en bas de page

1 Le recours à un « élément connu » (comme un mot de passe ou un numéro d’identification personnel [NIP]) comme facteur d’activation pour l’authentification multifactorielle (AMF) ne fait pas partie du champ d’application des présentes lignes directrices. Les mots de passe à facteur d’activation sont généralement moins dépendants de la longueur, ce qui signifie qu’ils ne nécessitent pas un minimum de 12 caractères. Cependant, ils doivent toujours être protégés contre les attaques par force brute étant donné que les mots de passe sont stockés localement.

2 La recommandation de 15 caractères repose sur les recommandations énoncées dans le document de Microsoft intitulé Vue d’ensemble technique des mots de passe.

ISBN : 978-0-660-79023-7

Date de modification : 2025-12-08

xx
yy