

# Etes-vous vulnérable au piratage?



## À quelle fréquence réutilisez-vous le même mot de passe pour différents comptes?

- A Toujours, car je peux facilement m'en souvenir.
- B Parfois, pour les comptes qui ne contiennent pas d'informations financières, privées ou sensibles.
- C Jamais. J'utilise des mots de passe uniques pour tous mes comptes et je les enregistre dans un gestionnaire de mots de passe.



## Quel est le niveau de complexité de vos mots de passe?

- A J'utilise toujours le même mot de passe et je change parfois le chiffre ou le symbole qu'il contient.
- B Je crée souvent des mots de passe uniques en mélangeant des lettres majuscules et minuscules, des chiffres et des symboles, surtout pour les comptes importants.
- C Je crée toujours des mots de passe uniques pour chaque compte en mélangeant des lettres majuscules et minuscules, des chiffres et des symboles, ou alors je crée des phrases de passe comprenant au moins quatre mots aléatoires.

## Quelle est la longueur de vos mots de passe?

- A Moins de 8 caractères
- B 8 à 10 caractères
- C Au moins 12 caractères pour un mot de passe ou 15 caractères pour une phrase de passe

## Notation

A = 1 point

B = 2 points

C = 3 points

## Calculez vos points.

## Résultats

### 6 à 10 points : Vos informations pourraient être compromises.

En ce moment, si vous réutilisez les mêmes identifiants de connexion, vos comptes sont exposés à un risque accru de piratage. Poser de petits gestes, comme éviter les informations personnelles dans vos mots de passe et activer l'authentification multifactorielle (AMF) dès que vous en avez l'occasion, peut faire une énorme différence.

Trouver le bon gestionnaire de mots de passe pourrait aussi vous aider en vous permettant de créer des mots de passe uniques et robustes pour chaque compte - ça pourrait vous éviter bien des maux de tête un jour! Vous n'aurez qu'un seul mot de passe à mémoriser pour accéder au gestionnaire (c'est plus facile que de se souvenir de dizaines de mots de passe différents). Il se chargera ensuite de tout mémoriser à votre place. Allez, vous pouvez y arriver!

### 11 à 15 points : Transformez vos bonnes habitudes en habitudes excellentes.

Vous êtes sur la bonne voie, mais vous pouvez encore vous améliorer! Poser de petits gestes peut faire une grande différence, comme utiliser un gestionnaire de mots de passe qui vous permet de créer des mots de passe uniques pour tous vos comptes (même ceux qui ne contiennent pas d'informations financières). Et n'oubliez pas d'activer l'authentification multifactorielle (AMF) dès qu'elle vous est proposée. Poursuivez votre route vers la sécurité!

Puisque vos comptes contiennent beaucoup d'informations personnelles, il est important de savoir comment les protéger. Répondez à ce questionnaire pour découvrir le niveau de sécurité de vos comptes et les habitudes que vous devriez adopter pour les rendre encore plus sûrs.

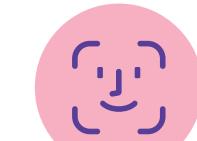
## Vos mots de passe contiennent-ils parfois des informations personnelles, comme des noms, des dates d'anniversaire, des noms d'animaux domestiques, etc.?

- A J'inclus toujours des informations personnelles, car elles sont plus faciles à mémoriser.
- B J'utilise parfois des informations personnelles, mais seulement si je sais que personne ne les connaîtra en ligne.
- C Je n'utilise jamais d'informations personnelles.



## Utilisez-vous l'authentification multifactorielle (AMF)?

- A Je ne sais pas exactement ce qu'est l'AMF.
- B Je l'utilise pour les comptes importants, comme les services bancaires en ligne, mais pas pour tous mes comptes.
- C J'active l'AMF dès qu'elle est offerte.



## Utilisez-vous un gestionnaire de mots de passe?

- A Non, mais il m'arrive parfois de noter mes mots de passe pour m'en souvenir.
- B Parfois, mais je n'utilise que celui qui est intégré à mon navigateur.
- C Oui, j'utilise un gestionnaire de mots de passe gratuit ou payant pour enregistrer tous mes identifiants uniques.



## \*\*\*\*\*

## \*\*\*\*\*

## Calculez vos points.

### 16 à 18 points : Vous êtes un as de la cybersécurité!

Vous avez de bonnes habitudes et vos comptes sont bien protégés. Continuez sur cette voie en restant à l'affût des nouvelles pratiques en matière de sécurité pour garder une longueur d'avance sur les cybermenaces. Si vous n'avez pas obtenu 18 points, concentrez-vous sur les points à améliorer. Bravo!

## Des conseils simples pour protéger vos comptes

- ★ Utilisez des mots de passe aléatoires et uniques pour chaque compte, ou utilisez des phrases de passe qui sont plus sûres et plus faciles à mémoriser.
- ★ Enregistrez vos identifiants dans un [gestionnaire de mots de passe](#) pour simplifier l'organisation. Vous n'aurez qu'un mot de passe principal à mémoriser pour accéder à votre compte.
- ★ L'AMF est très efficace pour prévenir le piratage de compte (article en anglais). Assurez-vous de l'activer chaque fois qu'on vous invite à le faire.
- ★ Mettez à jour vos anciens mots de passe, surtout s'ils contiennent des informations personnelles. [Apprenez à améliorer vos mots de passe en les remplaçant par des phrases de passe.](#)



Obtenez plus de conseils pour vous protéger et protéger vos appareils à



Centre de la sécurité des  
télécommunications Canada

Communications Security  
Establishment Canada

PENSEZ CYBERSECURITE.CA

Canada