GESTIONNAIRE DE MOTS DE PASSE


Login
Next Time Please
123456

L'erreur la plus courante d’une majorité de la population:

utiliser le même mot de passe sur tous ses comptes.

De cette manière, un hacker peut avoir accès à l'ensemble de votre vie informatique.

Vous avez quelques options:

- **Vous continuez avec vos mots de passe usuels**:
  - **vous les connaissez par cœur ou sauvegarder sur un bout de papier**;
  - **Risque très élevé**.
- **Il y a la méthode « Diceware »**.
  - **Risque potentiel**.
- **Il y a la méthode dite « phonétique »: risque minime (secret)**

Exemple: **"J'ai acheté huit CD pour cent euros cet après-midi"** = ght8CD%E7am

- **Il y a la méthode dite « des premières lettres » risque minime (secret)**

Exemple: **"Un tien vaut mieux que deux tu l'auras"** = 1tvmQ2tl'A

Et d’autres… la « passephrase »

Vous pouvez choisir quelques lignes d’une chanson ou d’un poème et utiliser la première lettre de chaque mot.

Par exemple, « *In Xanadu did Kubla Kahn a stately pleasure dome decree!* » devient « IXdKKaspdd! ». Vous pouvez également utiliser une phrase de passe longue composée de l'ensemble des mots collés les uns aux autres. (InXanaduDidKublaKahnAStatelyPleasureDomeDecree!). Facile à retenir, avec une résistante importante et déclinable pour générer autant de mots de passe/passephrases que nécessaire.

Si vous désirez créer & gérer vos mots de passe vous-même:

- Un bon mot de passe est un mot de passe long qui ne sert que sur un compte et qui ne vous identifie pas.
- L'utilisation de longues phrases, faciles à retenir, au détriment des mots de passe à chiffres et caractères spéciaux.

Pourquoi utiliser un gestionnaire de mots de passe ?

- Il ne s'agit évidemment pas d'une obligation.
- En fait, l'immense majorité des utilisateurs s'en passe.
- Il permet cependant de répondre à des problématiques qui peuvent paraître simples, mais qui surchargent rapidement de responsabilité toute personne désireuse de faire attention à la sécurité de ses comptes en ligne.

Est-ce compliqué
d'utiliser
un gestionnaire
de mots de passe ?

Choisir un bon mot de passe est une science complexe qui fait l'objet de recommandations sans cesse renouvelées... et bien souvent contradictoires.

Créer un mot de passe en 2018

- RECOMMENDATION:

- 12 MULTI CARACTÈRES ET PLUS.

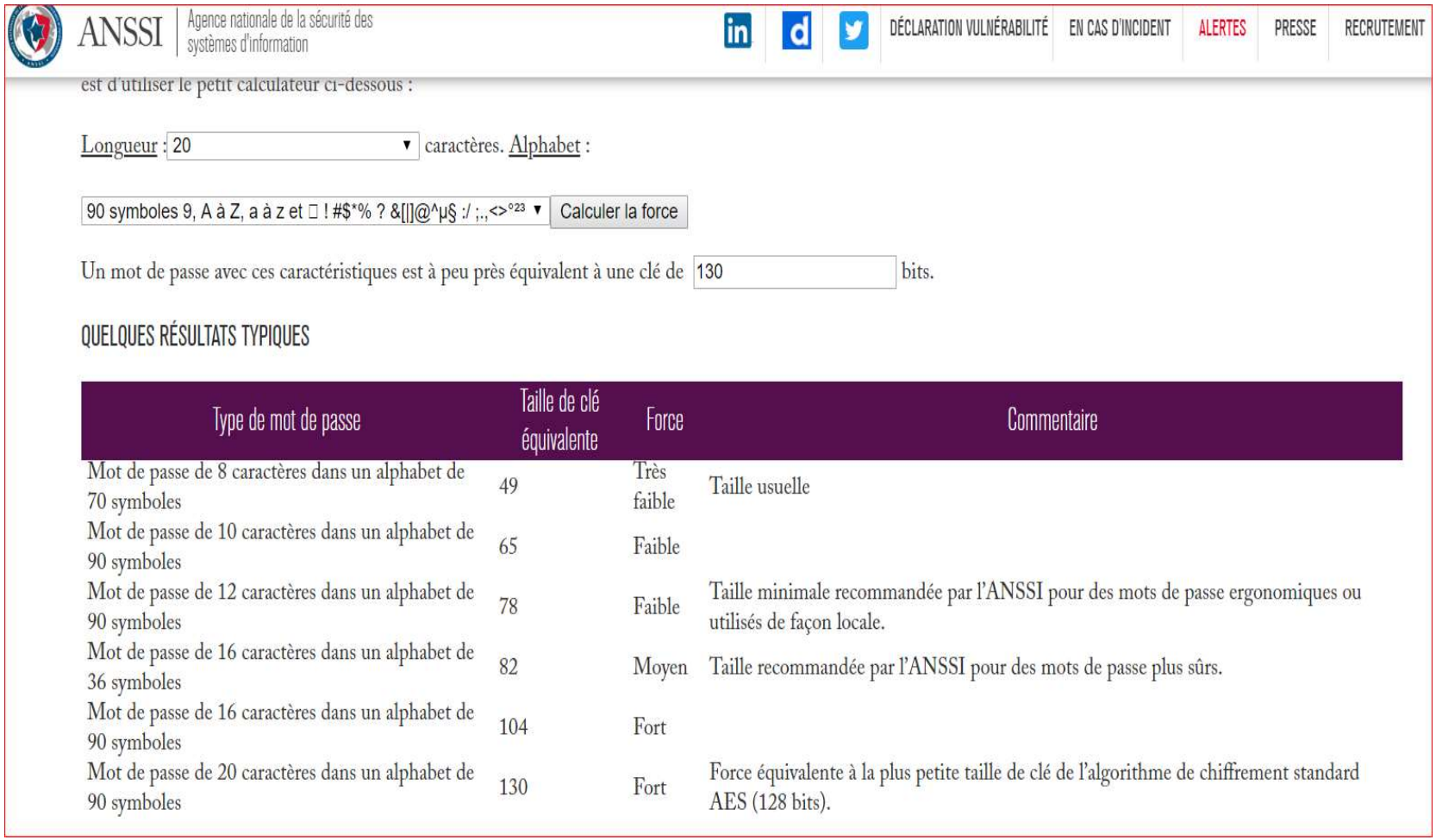
Un mot de passe est confronté globalement à deux problèmes majeurs :

- son degré de force;
- sa réutilisation.

Un bon mot de passe est long, complexe, n'utilise pas de séquence évidente (mots du dictionnaire, dates, noms, etc.), comprend des majuscules, minuscules, chiffres et caractères spéciaux.

Quant à la réutilisation, elle favorise le piratage en série des comptes : si des pirates trouvent votre mot de passe, ils pourront s'en servir sur d'autres services.

COMMENT RENFORCER UN MOT DE PASSE



ANSSI | Agence nationale de la sécurité des systèmes d'information

DÉCLARATION VULNÉRABILITÉ | EN CAS D'INCIDENT | ALERTES | PRESSE | RECRUTEMENT

est d'utiliser le petit calculateur ci-dessous :

Longueur : 20 ▾ caractères. Alphabet :

90 symboles 9, A à Z, a à z et □ ! #$*% ? &[|]@^µ§ :/ ;.,<>°²³ ▾ Calculer la force

Un mot de passe avec ces caractéristiques est à peu près équivalent à une clé de 130 bits.

QUELQUES RÉSULTATS TYPIQUES

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

- Avec l'exemple correcthorsebatterystaple , l'outil détecte bien qu'il s'agit de quatre mots collés les uns aux autres et indique qu'il faudrait 8 heures à un ordinateur capable de traiter 10 milliards d'opérations par seconde…

…alors qu'il ne faudrait que 10 secondes pour

Tr0ub4dor&3

- Si l'on prend l'exemple de la formule sin^2(x)+cos^2(x)=1

le temps de traitement passe à 31 ans

...alors qu'il faudrait des siècles pour venir à bout de la passephrase:

InXanaduDidKublaKahnAStatelyPleasureDomeDecree


En 2017, prends la résolution
de te protéger sur Internet
Gab
Gagnon.ca

- Créer un mot de passe fort pour chaque site devient vite éprouvant.
- C’est ici que les gestionnaires entrent en piste, d’autant que beaucoup proposent une intégration directe dans le navigateur.
- L’utilisateur peut générer des mots de passe forts de manière aléatoire, en un clic, une extension le connectant automatiquement quand il revient sur le site.

Interface et prise en main

- L'interface, l'ergonomie, la facilité de prise en main ont longtemps été les parents pauvres de la conception logicielle.
- Ce sont pourtant ces réalisations qui déterminent l'efficacité d'utilisation, qui font qu'un utilisateur pourra utiliser aisément une solution.
- La « courbe d'apprentissage » d'une application peut faire toute la différence.

- Autant le dire : *gérer ses mots de passe ne fait rêver personne.*
- Il ne s'agit pas ici d'un jeu ou même de n'importe quel autre logiciel qui revêtirait un aspect divertissant ou récréatif.
- Pour de nombreux utilisateurs, un mot de passe est pénible à générer et à retenir.


Pourquoi j'utilise un
gestionnaire de mots de passe ?

Les meilleurs gestionnaires de mots de passe testés en 2018

- Dashlane
  Site Web: https://www.dashlane.com
- LastPass
  Site Web: https://www.lastpass.com/fr
- KeePass
  Site Web: https://www.keepass.fr
- 1Password
  Site Web: https://1password.com/fr
- Keeper
  Site Web: https://keepersecurity.com/fr

Après analyse, j’ai fait l’acquisition de Dashlane

Version Gratuite de Dashlane

- Gérez jusqu'à 50 mots de passe;

et remplissez automatiquement l'ensemble de vos informations personnelles sur votre appareil préféré, gratuitement et à vie.

- Stockage sécurisé des mots de passe;

- Dashlane sur un appareil;

- Saisie automatique des données personnelles et des informations de paiement;

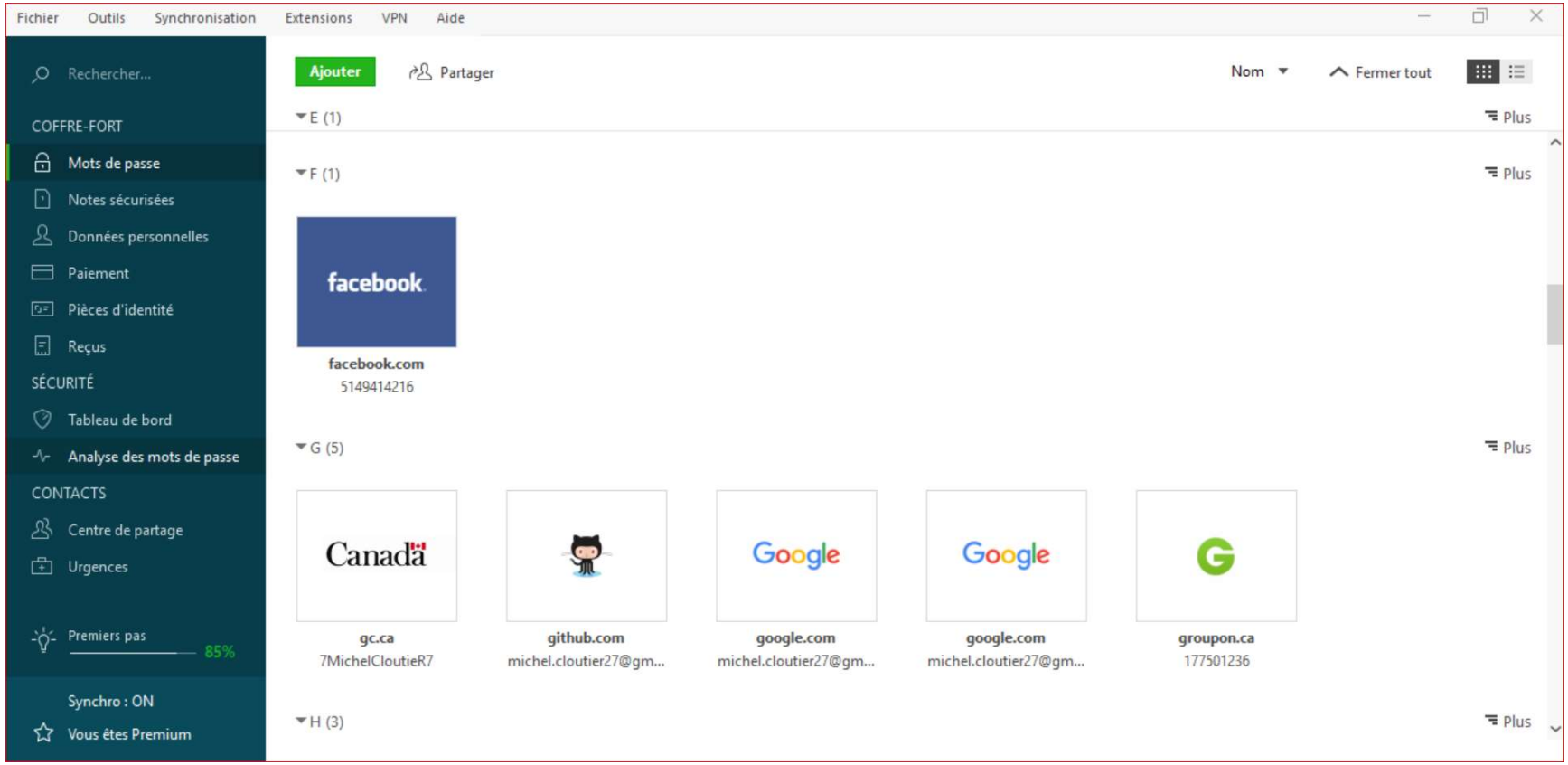
- Alertes de sécurité.

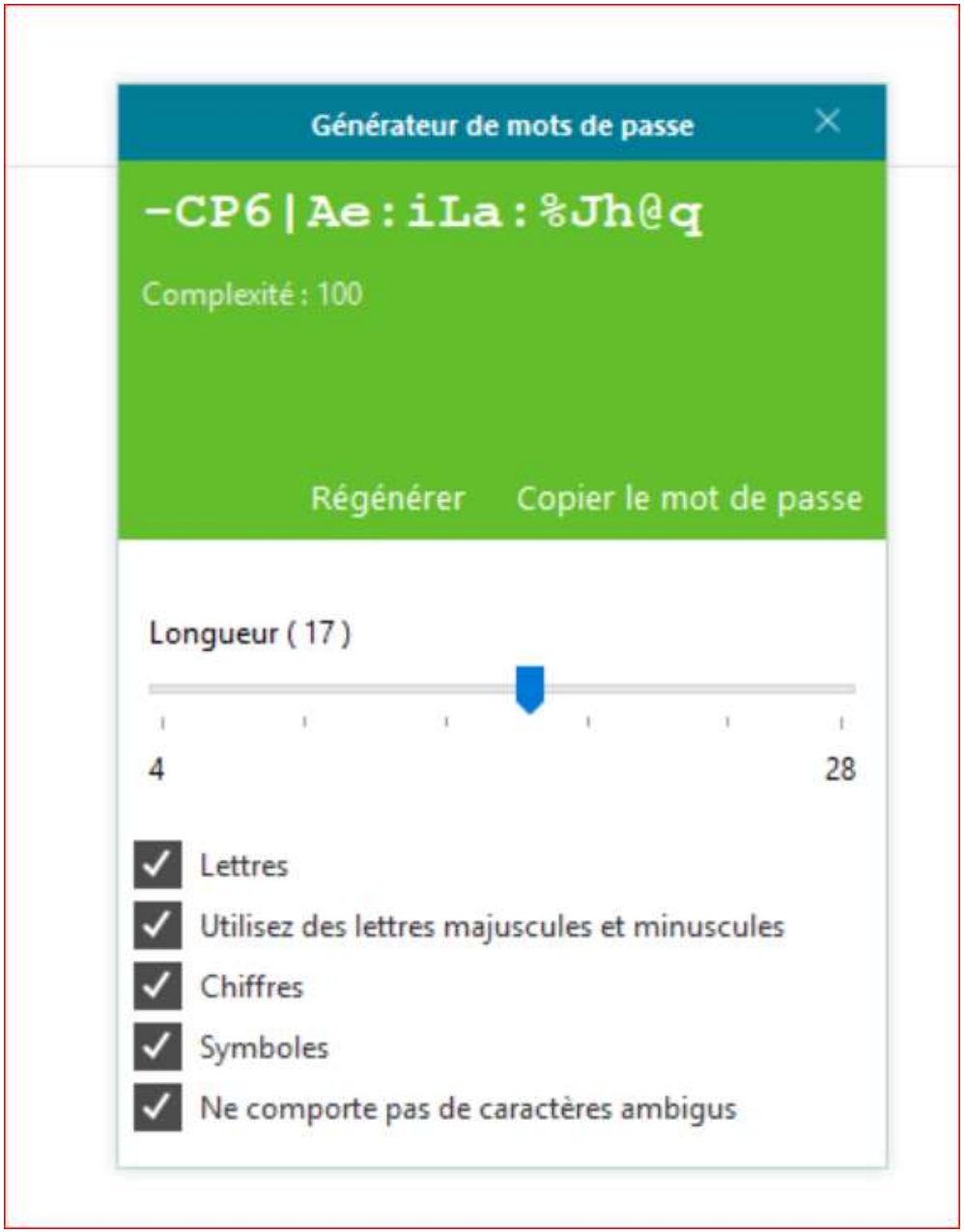
Version « Premium »

Coût annuel: 53,47$CAD / an

- Gérez un nombre illimité de mots de passe;
- Sur autant d'appareils que vous le souhaitez;
- Et bénéficiez en plus de la surveillance du Dark Web;
- Ainsi que d'un VPN sécurisé.


89.0%
3%
3%
0.8%
0.8%


Fichier
Outils
Synchronisation
Extensions
VPN
Aide
Rechercher...
COFFRE-FORT
Mots de passe
Notes sécurisées
Données personnelles
Paiement
Pièces d'identité
Reçus
SÉCURITÉ
Tableau de bord
Analyse des mots de passe
CONTACTS
Centre de partage
Urgences
Premiers pas
85%
Synchro : ON
Vous êtes Premium
Ajouter
Partager
Nom
Fermer tout
E (1)
Plus
F (1)
Plus
facebook
facebook.com
5149414216
G (5)
Plus
Canada
gc.ca
7MichelCloutieR7
github.com
michel.cloutier27@gm...
Google
google.com
michel.cloutier27@gm...
Google
google.com
michel.cloutier27@gm...
groupon.ca
177501236
H (3)
Plus


Générateur de mots de passe
-CP6|Ae:iLa:%Jh@q
Complexité : 100
Régénérer
Copier le mot de passe
Longueur (17)
4
28
Lettres
Utilisez des lettres majuscules et minuscules
Chiffres
Symboles
Ne comporte pas de caractères ambigus

C’est pas « automatique »

Lorsque vous vous inscrivez en ligne, vous devrez:

Créer un mot de passe « maître »:

- Soit crée par vous ou via le générateur de mots de passe;
- Le seul mot de passe à noter et se souvenir, que vous pourrez changer.

Enregistrer sur le site du gestionnaire, tous les sites Web, applications, extensions que vous utilisez et pourrez modifier vos mots de passe « faibles ».

Gestion du mot de passe maître : pas de solution miracle en cas de perte

- Un mot de passe maître/central qui doit être particulièrement fort.
- En théorie, il doit s'agir du seul qu'il faut vraiment retenir puisque les autres peuvent être consultés sur votre compte.
- Une règle est valable dans tous les cas : il ne faut jamais perdre le mot de passe maître.
- Il n'existe pas de fonction de récupération

Verdict :
il faut définir ses priorités avant de décider

Les gestionnaires de mots de passe…

pour éviter de devoir…

en mémoriser des dizaines

Michel Cloutier, pour les VBDL, 20181017