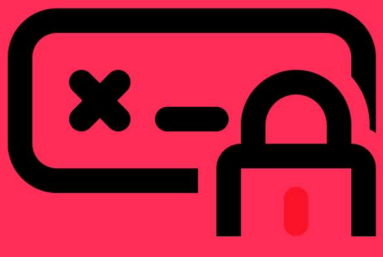
J'utilise des mots de passe forts



Je renforce mes mots de passe

Je protège ma vie privée

01

Pourquoi
utiliser un mot de passe fort ?

Pour protéger mes comptes :
Un mot de passe fort empêche les hackers d'accéder à tes informations personnelles, tes mails, ou tes réseaux sociaux.

Pour éviter le vol d'identité :
Si quelqu'un vole ton mot de passe, il peut se faire passer pour toi.

Pour sécuriser tes données sensibles :
Autant tes informations bancaires ou professionnelles.

Pour rendre la tâche difficile aux pirates :
Un mot de passe simple peut être deviné ou cassé rapidement avec des outils automatiques.

Pour garder le contrôle de tes comptes :
Personne d'autre ne pourra changer tes paramètres ou accéder à tes services.

- *Attaque par dictionnaire*
  Le pirate teste des mots de passe courants ou trouvés dans des listes de mots (comme « 123456 », « password », « qwerty »).

- *Phishing (hameçonnage)*
  Le pirate t'envoie un faux message pour te faire entrer ton mot de passe sur un site qui ressemble au vrai.

02

Comment
créer un mot de passe fort

- Utilise au moins 12 caractères
- Ajoute des chiffres
- Ajoute des symboles comme ! @ # ?
- Évite les mots courants et les infos personnelles (nom, date de naissance)
- Utilise une phrase ou un groupe de mots faciles à retenir mais difficiles à deviner

- *Exemple :*

  Soleil@Lune#42!
  Chat$Nuage%Fleur
  *Pizza*Bleu&Cerise7*

03

.

Avantages
a utiliser un gestionnaire de mots de passe

Mot de passe fort à chaque fois
Il crée automatiquement des mots de passe longs et complexes, difficiles à deviner.

Plus besoin de retenir tous tes mots de passe
Tu n'as qu'un seul mot de passe maître à retenir. Le reste est stocké en sécurité.

Remplissage automatique
Il peut remplir tes identifiants à ta place, plus rapide et pratique.

Alerte en cas de mot de passe compromis
Certains te préviennent si un de tes mots de passe a été piraté.

Pas de réutilisation dangereuse
Il t'aide à avoir un mot de passe différent pour chaque site (et donc à mieux te protéger).

Disponible partout
La plupart fonctionnent sur ordinateur, tablette et téléphone, avec synchronisation entre les appareils.

Conseils de prévention

Pourquoi utiliser le 2FA
(authentification à deux facteurs)

Plus de sécurité
Même si quelqu'un vole ton mot de passe, il ne pourra pas se connecter sans le deuxième facteur (ex. : code SMS, appli, empreinte digitale).
Protège contre le piratage
Le 2FA empêche les hackers d'accéder à tes comptes, même s'ils trouvent ton mot de passe avec une attaque ou un phishing.
Facile à utiliser
Tu reçois juste un code par SMS ou via une appli (comme Google Authenticator ou Microsoft Authenticator).
Recommandé par les experts
Les sites les plus sécurisés (banques, mails, réseaux sociaux) l'utilisent et te le proposent.
Fonctionne partout
Tu peux l'activer sur presque tous tes comptes : Gmail, Facebook, Instagram, Amazon, etc.

Pour toutes questions ou suggestions d’amélioration.

ubik-infosec.ca @michel-panouillot

A propos de l’auteur

Professionnel chevronné en sécurité de l'information, je cumule plus de dix ans d’expérience dans des environnements complexes et diversifiés, incluant les secteurs gouvernementaux, de la formation et militaire. Mon expertise est centrée sur l’analyse en cybersécurité, avec une spécialisation en gouvernance et conformité réglementaire.