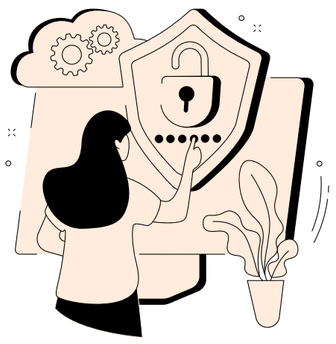
Bonnes pratiques en Cybersécurité

Document réalisé par Culture Saguenay - Lac-Saint-Jean

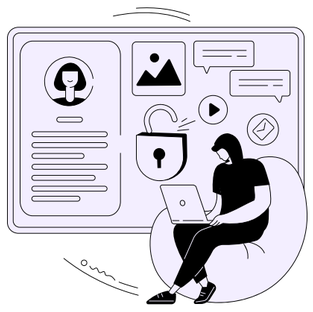
5 ETAPES POUR MIEUX GERER SES MOTS DE PASSE

Pourquoi la gestion des mots de passe est-elle critique ?



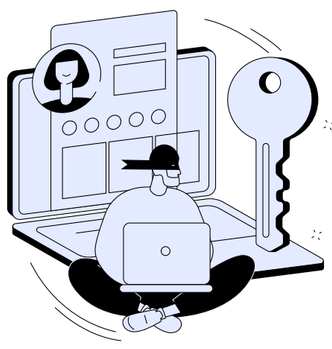
- Premier rempart contre les intrusions
- 81% des violations de données sont liées aux mots de passe compromis
- Un mot de passe faible met tout en danger

1 Règles d'or pour créer un mot de passe sécurisé



- Longueur : 12 à 16 caractères
- Complexité : majuscules, minuscules, chiffres, symboles
- Aucune information personnelle
- Utiliser une phrase secrète mémorisable
- Phrase codée : 'Mon premier vélo date de 2007!' -> 'Mpvd@2007!'
- Associer à une histoire imagée pour mieux retenir

2 Techniques pour mieux gérer ses mots de passe



- Utiliser un gestionnaire (Bitwarden, 1Password, KeePass, DashLane)
- Activer l'authentification multifacteur (MFA)
- Séparer les mots de passe par usage
- Changer régulièrement

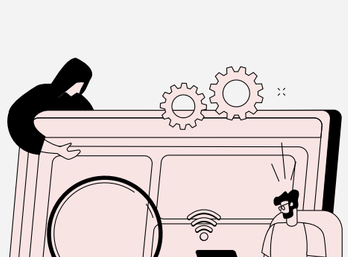
3 Bonnes pratiques pour les professionnels

- Mettre en place une politique de mot de passe (longueur, complexité)
- Former les utilisateurs
- Surveiller les comptes pour détecter les mots de passe compromis

Outils recommandés

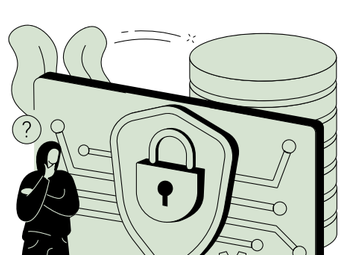
- Tester un mot de passe : www.security.org/how-secure-is-my-password/
- Vérifier une compromission : haveibeenpwned.com
- Générer des mots de passe : via gestionnaire

4 En cas de mot de passe compromis



- Changer immédiatement le mot passe et les mots de passe similaires
- Vérifier les autres comptes
- Activer le MFA
- Informer l'équipe sécurité
- Verifier les activités suspectes

5 Ce qu'il faut éviter



- Utiliser des mot de passe trop evident
- Réutiliser le même mot de passe
- Noter sur post-it
- Envoyer par email/SMS non sécurisé
- Stocker en clair dans un fichier.
- Apprendre de l’incident