

# CHOISIR UN MOT DE PASSE ROBUSTE



Les acteurs malveillants peuvent utiliser une attaque de type « force brute », consistant à essayer toutes les combinaisons possibles jusqu'à trouver le bon mot de passe. Votre mot de passe doit donc être suffisamment long et complexe afin qu'il ne puisse pas être trouvé.



## LES BONS REFLEXES

- 1 Utilisez une combinaison d'au minimum 12 caractères, mélangeant les minuscules, les majuscules, les chiffres et les caractères spéciaux.
- 2 N'utilisez pas de lettres ou nombres séquentiels comme 123456, qwertz, abcdef, etc.
- 3 L'utilisation de moyens mnémotechniques est recommandée pour un mot de passe facilement mémorisable :
  - ▶ **La méthode des initiales**
    - Phrase : « 2 vélos sont nécessaires pour des vacances de 30 jours »
    - Mot de passe : « 2VsnpdVd30j! »
  - ▶ **La méthode phonétique**
    - Phrase : « Elle aime beaucoup cette cassette et cette bande dessinée »
    - Mot de passe : « Lmbcp7k7&7BD »
  - ▶ **Votre propre méthode personnelle !**
- 4 N'utilisez pas d'informations personnelles comme votre date de naissance, le prénom de votre enfant, votre groupe de musique préféré, etc.
- 5 N'utilisez pas des noms ou des mots du dictionnaire.



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Haut-Commissariat  
à la protection nationale

Agence nationale de la sécurité  
des systèmes d'information