15 minutes d'avance

Fiche conseil. 05

Comment construire un bon mot de passe ?

Entre nos comptes professionnels et nos comptes personnels, chacun de nous est amené à mémoriser près de 80 mots de passe. Pas étonnant que nous les choisissions simples, courts et ... similaires !

Sans surprise, une étude de Verizon en 2021 montre que 81% des violations sont issues de mots de passe faibles ou compromis. Forte de ce constat, en octobre 2022, la Cnil a procédé à une mise à jour de ses recommandations relatives aux mots de passe et autres secrets partagés.

Risques

Un mot de passe cracké, c'est une ouverture sur les applications et sur les données qu'elles hébergent :

1. Menaces sur la sécurité des données : **perte de confidentialité**.
2. Piratage des comptes : **perte d'intégrité, perte d'authenticité**.
3. Attaque de rançongiciel : **perte de disponibilité, menaces**.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité
- Art. 32 sur l'obligation d'assurer la sécurité des données personnelles

Selon la Cnil, le mot de passe n'est pas la meilleure solution mais la plus répandue. C'est pourquoi elle propose ses recommandations sous forme de dispositif de droit souple, et non d'obligations.

Pour aller plus loin (ex. authentification multi-facteurs) se référer au guide l'Anssi sur l'authentification.

Bonnes pratiques

- **Créer un mot de passe fort** : préférer la complexité (robustesse) au nombre de caractères ; La Cnil établit ses recommandations en degré d'entropie (voir : calcul d'entropie)
  - mixer les langues (pour éviter les attaques par dictionnaire) ;
  - mixer les mots qui n'ont pas de lien entre eux ;
  - proscrire les informations personnelles : date de naissance, prénoms des enfants, plaque d'immatriculation (pour contourner les attaques par ingiénerie sociales) ;
  - mixer minuscules, majuscules, chiffres et caractères spéciaux ;
  - créer des phrases de passe ;
  - permuter les caractères : a > @, de > 2, ien > 1 ;
  - utiliser les initiales de chaque mot d'une phrase ;
  - éviter les é, à, â, ü qui ne sont pas disponibles sur tous les claviers ; ...

Solution = **MIXER + ÊTRE INVENTIF + ÊTRE CRÉATIF** à défaut, utiliser le générateur de mot de passe de la Cnil.

- **Mémoriser / stocker ses mots de passe** : confier ses mots de passe à un gestionnaire de mot de passe (ex. KeePass, recommandé par la Cnil et l'Anssi). Le coffre-fort numérique évite de noter en clair ou de mémoriser et permet de ne retenir qu'un seul mot de passe (mot de passe "maître").
- **Mettre à jour ses mots de passe** : la Cnil abandonne le renouvellement périodique (finalement contre-productif) au profit de mots de passe robustes. Si vos mots de passe sont robustes et protégés en coffre-fort, il n'est plus nécessaire de les changer régulièrement.
- **Notifier** son DPO en cas de violation.

Ex. P@ssw0rd!2023

Ex. M0nM0t2P@ssE!

Pour aller plus loin

Recommandations Cnil (oct. 2022)

ANSSI – guide de l'authentification (2021)

KEEPASS coffre-fort