Longueur du mot de passe	Seulement des chiffres	Lettres minuscules	Mélange de minuscules et majuscules	Mélange de minuscules-majuscules et de chiffres	Mélange de minuscules-majuscules, de chiffres et de symboles
3	Instantané	Instantané	Instantané	Instantané	Instantané
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	Instantané	Instantané	Instantané
6	Instantané	Instantané	Instantané	Instantané	Instantané
7	Instantané	Instantané	2 s	7 s	31 s
8	Instantané	Instantané	2 mn	7 mn	39 mn
9	Instantané	10 s	1 heures	7 heures	2 jours
10	Instantané	4 mn	3 jours	3 semaines	5 mois
11	Instantané	2 heures	5 mois	3 ans	34 ans
12	2 s	2 jours	24 ans	200 ans	3.000 ans
13	19 s	2 mois	1.000 ans	12.000 ans	202.000 ans
14	3 mn	4 ans	64.000 ans	750.000 années	16.000.000 années
15	32 mn	100 ans	3.000.000 années	46.000.000 années	1.000.000.000 années
16	5 heures	3.000 ans	173.000.000 années	3.000.000.000 années	92.000.000.000 années
17	2 jours	69.000 ans	9.000.000.000 années	179.000.000.000. années	7.000.000.000.000 années
18	3 semaines	2.000.000 années	467.000.000.000 années	11.000.000.000.000 années	438.000.000.000.000 années

Source : Étude sur la robustesse des mots de passe et du temps qu'il faut pour les casser en 2022 – Verspieren

10 RÉFLEXES INCONTOURNABLES POUR RENFORCER VOTRE POLITIQUE DE GESTION DES MOTS DE PASSE

1. Utilisez des mots de passe uniques (différents pour chaque accès) et solides :
   - choisissez des mots de passe de minimum 12 caractères ;
   - privilégiez des mots n'existant pas dans le dictionnaire ;
   - évitez les informations qui vous concernent ou facilement accessibles sur les réseaux sociaux par exemple ;
   - utilisez des caractères spéciaux et des chiffres.
2. Activez la double authentification chaque fois que possible.
3. Renouvelez-les tous les 2 ou 3 mois.
4. Ne stockez jamais vos mots de passe de manière accessible.
5. N'activez pas l'option "mémorisez vos mots de passe".
6. Ne communiquez jamais vos mots de passe, pas même à un proche collaborateur pour lui faciliter l'accès à un dossier partagé.
7. N'utilisez pas d'autres comptes que le vôtre.
8. Disposez d'une procédure pour gérer le départ des collaborateurs (changement des mots de passe systématique, suppression de leurs accès...).
9. Utilisez des coffres-forts virtuels : Keepass (référencé par l'ANSSI)...
10. Au moindre doute, changez votre mot de passe.

Et surtout, sensibilisez vos collaborateurs à l'ensemble de ces bonnes pratiques pour qu'ils aient un comportement responsable et avisé.

POUR EN SAVOIR PLUS

Vous pouvez consulter les outils mis à disposition par l'Ordre des experts-comptables sur www.experts-comptables.fr (partie privée) :

- Kit Mission Cyber
- Le guide de la cybersécurité pour les experts-comptables
- 11 commandements pour se prémunir de la cybercriminalité
- Fiche Info client : les principales étapes en cas de cyberattaque
- Voir également l'infographie « 10 conseils pour sécuriser vos données et celles de vos clients », p.45