

Mots de passe : les bonnes pratiques en entreprise

Longueur, unicité, gestionnaire de mots de passe : comment mettre fin au post-it sous le clavier.

12 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/mots-de-passe

Plus de 80 % des intrusions exploitent des mots de passe faibles, réutilisés ou volés. C'est la porte d'entrée numéro un des attaquants — et l'une des plus simples à verrouiller. Ce guide fait le tour complet du sujet : comment les attaquants s'y prennent, ce qui fait un mot de passe réellement robuste, comment déployer un gestionnaire dans une équipe, et quelle politique fixer noir sur blanc dans l'entreprise.

1. Comment les attaquants s'y prennent

Comprendre l'attaque aide à choisir la bonne défense. Les mots de passe se font voler de quatre grandes manières :

- Les fuites de données : un site sur lequel vous aviez un compte se fait pirater, et votre couple email + mot de passe se retrouve en vente. Si vous réutilisez ce mot de passe ailleurs, tous vos comptes tombent (attaque dite de « credential stuffing »)
- Le phishing : une fausse page de connexion vous fait saisir vos identifiants vous-même
- La force brute : des machines testent des millions de combinaisons par seconde contre un compte exposé ou un fichier volé
- Le vol direct : post-it, fichier Excel sur le serveur, mot de passe tapé devant témoin ou envoyé par email

CAS CONCRET

Un mot de passe de 8 caractères, même avec majuscules et chiffres, se casse aujourd'hui en quelques heures avec du matériel grand public. Le même en 14 caractères demande des siècles. La longueur n'est pas un détail : c'est LE facteur.

2. Ce qui fait un bon mot de passe

Contrairement à une idée reçue, la longueur compte plus que la complexité. Une phrase de passe de 4 à 5 mots aléatoires (ex. « cheval-orage-piano-73-lune ») est à la fois plus robuste et plus facile à retenir que « P@ssw0rd! », que tous les outils de cassage testent en premier.

- Au moins 14 caractères (l'ANSSI recommande 12 minimum, visez plus)
- Un mot de passe différent pour chaque service — sans exception : c'est la parade au credential stuffing
- Jamais d'information personnelle : date de naissance, prénom des enfants, nom de l'entreprise — tout cela figure sur vos réseaux sociaux
- Jamais le même mot de passe pro et perso : une fuite sur un forum de loisirs ne doit pas ouvrir votre messagerie professionnelle
- Pas de motif prévisible : « Entreprise2026! » et les suites de clavier (azerty123) sont dans tous les dictionnaires d'attaque

3. Le gestionnaire de mots de passe : indispensable

Personne ne peut retenir 50 mots de passe uniques et longs. Le gestionnaire résout cette impossibilité : il génère, stocke chiffrés et remplit automatiquement tous vos mots de passe. Vous n'en retenez plus qu'un seul — le mot de passe maître — et il doit être exceptionnel.

Choisir l'outil

- Bitwarden : open source, audité, version gratuite solide et offre entreprise abordable — notre recommandation par défaut
- KeePass (et variantes KeePassXC) : gratuit, hors ligne, certifié par l'ANSSI — idéal si vous refusez le cloud, mais moins pratique en équipe
- 1Password, Dashlane, Proton Pass : très aboutis, offres famille et entreprise
- Les gestionnaires intégrés aux navigateurs dépannent, mais offrent moins de contrôle (partage, audit, départ d'un salarié)

Le déployer en équipe

- Prendre une offre « business » : coffres partagés par service, administration centrale, révocation immédiate d'un compte
- Migrer progressivement : commencer par les comptes critiques (banque, messagerie, admin), puis le reste au fil de l'eau
- Former chacun 20 minutes : installation, extension navigateur, application mobile, génération d'un mot de passe
- Interdire explicitement les anciens stockages (fichier Excel, carnet, navigateur perso) une fois la migration faite

Le mot de passe maître et la récupération

Le mot de passe maître est le seul à retenir : faites-en une phrase de passe de 5 mots minimum, jamais écrite en clair, jamais réutilisée. Prévoyez aussi la récupération : la plupart des gestionnaires proposent un kit d'urgence (code de récupération à imprimer et stocker en lieu sûr, par exemple dans un coffre physique) et, en version entreprise, une récupération administrateur. Sans cela, un mot de passe maître oublié signifie un coffre définitivement perdu.

4. Quelle politique fixer dans l'entreprise

Les bonnes pratiques individuelles ne tiennent que si l'entreprise les cadre. Une politique de mots de passe tient en une demi-page de la charte informatique :

- Gestionnaire d'entreprise obligatoire pour tout identifiant professionnel
- 14 caractères minimum, générés par le gestionnaire
- Un compte nominatif par personne — les comptes génériques (« accueil », « compta ») sont supprimés ou convertis en coffres partagés
- Transmission d'identifiants uniquement via le partage sécurisé du gestionnaire, jamais par email, SMS ou messagerie instantanée
- Double authentification obligatoire sur messagerie, banque, comptes administrateurs et accès distants
- Au départ d'un collaborateur : révocation de son compte gestionnaire et rotation des mots de passe des coffres auxquels il avait accès

ATTENTION

Le renouvellement forcé tous les 90 jours est une pratique dépassée, abandonnée par l'ANSSI comme par le NIST : il pousse aux variantes prévisibles (« Hiver2025! » devient « Printemps2025! »). Un mot de passe long et unique se garde tant qu'il n'y a pas de soupçon de compromission — et se change immédiatement dès qu'il y en a un.

5. Détecter les fuites avant les attaquants

Vos mots de passe peuvent fuiter sans que vous y soyez pour rien : il suffit qu'un service que vous utilisez se fasse pirater. La bonne nouvelle : ces fuites se surveillent.

- haveibeenpwned.com : saisissez une adresse email et voyez dans quelles fuites connues elle apparaît ; le service permet aussi de surveiller tout un nom de domaine — précieux pour une entreprise
- Les gestionnaires de mots de passe intègrent des rapports de santé : mots de passe réutilisés, faibles ou présents dans des fuites, à traiter en priorité
- En cas d'alerte : changer le mot de passe concerné partout où il était utilisé, et activer la MFA sur le compte touché

6. Les erreurs à bannir

- Le fichier Excel « mots de passe.xlsx » sur le serveur partagé — première trouvaille de tout attaquant (et de tout audit)
- Le post-it sur l'écran ou sous le clavier
- L'envoi d'identifiants par email ou par SMS en clair : ils restent lisibles des années dans les historiques
- Le compte générique partagé par toute l'équipe : aucune traçabilité, jamais changé
- Les mots de passe jamais changés après le départ d'un collaborateur
- Le mot de passe « temporaire » (Bienvenue2026!) jamais remplacé par l'utilisateur

L'essentiel à retenir

- 01 Déployer un gestionnaire de mots de passe pour toute l'équipe
- 02 Imposer 14 caractères minimum, générés par le gestionnaire
- 03 Faire du mot de passe maître une phrase de passe et prévoir sa récupération
- 04 Supprimer les comptes génériques partagés
- 05 Surveiller les fuites de données sur votre domaine (haveibeenpwned)
- 06 Changer tous les mots de passe auxquels un ex-collaborateur avait accès
- 07 Activer la double authentification partout où c'est possible

Questions fréquentes

Un gestionnaire de mots de passe, n'est-ce pas mettre tous ses œufs dans le même panier ?

Si — mais un panier blindé vaut mieux que cinquante paniers en carton. Les gestionnaires sérieux chiffrent le coffre localement : même leur éditeur ne peut pas lire vos données. Le risque résiduel (mot de passe maître faible ou volé) se couvre avec une phrase de passe solide et la double authentification sur le coffre. Toutes les autorités de sécurité, ANSSI comprise, recommandent leur usage.

Puis-je laisser mon navigateur retenir mes mots de passe ?

C'est mieux que de les réutiliser, mais insuffisant en entreprise : pas de partage sécurisé entre collègues, pas de révocation au départ d'un salarié, et un accès à la session du poste donne souvent accès aux mots de passe. Le gestionnaire dédié règle ces trois problèmes.

Comment transmettre un mot de passe à un collègue ou un prestataire ?

Par la fonction de partage du gestionnaire, qui chiffre de bout en bout et permet de retirer l'accès plus tard. À défaut, par un lien à usage unique et à expiration. Jamais par email ni messagerie : le mot de passe y reste lisible indéfiniment.

Que faire si un collaborateur oublie son mot de passe maître ?

Avec une offre entreprise, l'administrateur peut déclencher la procédure de récupération du compte. Sans cela, le coffre est perdu et il faut réinitialiser les mots de passe de tous les comptes qu'il contenait — c'est précisément pourquoi le kit de récupération se prépare au déploiement, pas le jour du problème.

Pour aller plus loin

ANSSI — Recommandations relatives aux mots de passe — cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

CNIL — Mots de passe : les bonnes pratiques — www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers

Have I Been Pwned — vérifier si une adresse a fuité — haveibeenpwned.com

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr