Sécuriser ses mots de passe en 2025

Guide pratique pour les TPE/PME

Pourquoi ce guide ?

Les mots de passe sont aujourd'hui la première porte d'entrée des cyberattaques. Une petite erreur suffit pour bloquer une entreprise entière.

Ce guide vous accompagne pas à pas pour protéger efficacement votre activité sans complexité technique.

Le problème en quelques mots

Piratage instantané

Les mots de passe trop simples se font pirater en quelques secondes grâce aux attaques automatisées.

Réutilisation dangereuse

Les mots de passe réutilisés explosent le risque : un seul compte compromis met tous les autres en danger.

Toutes les entreprises visées

Une TPE est aussi ciblée qu'un grand groupe. Les cybercriminels ne font pas de distinction.

Ce qu'il faut retenir sur les bons mots de passe

Plus ils sont longs, mieux c'est

La longueur est votre meilleure protection. Visez au minimum 12 caractères.

Les mélanges aident beaucoup

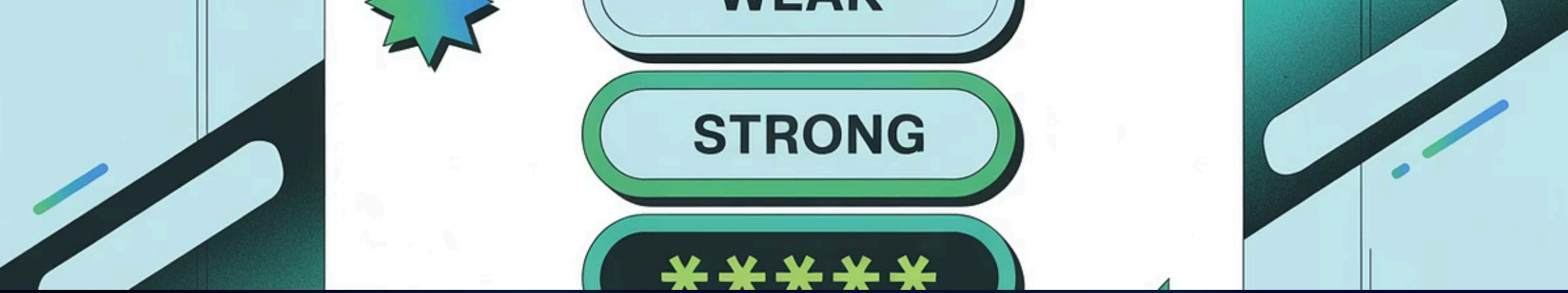
Combinez lettres majuscules, minuscules, chiffres et symboles pour une sécurité maximale.

Jamais le même deux fois

Chaque compte doit avoir son propre mot de passe unique. Aucune exception.

Évitez les informations personnelles

Pas de dates d'anniversaire, prénoms, noms d'animaux ou informations facilement devinables.



Exemples très concrets

❌ À éviter absolument

- 123456
- azerty
- Julie2024
- motdepasse
- admin123

✓ À privilégier

Une longue combinaison difficile à deviner, même si elle semble "bizarre".

Exemple : Jm@ng3D3sP0mm€s!2025

Une méthode facile pour créer un bon mot de passe

01

Choisir une phrase simple

Par exemple : "Je mange des pommes tous les matins"

02

Garder les premières lettres

Cela donne : Jmdptlm

03

Ajouter majuscules, chiffres et symboles

Transformez en : Jm@ng3D3sP0mm€s!2025

Résultat : Un mot de passe solide, impossible à deviner, mais facile à retenir grâce à votre phrase personnelle.

Pourquoi un gestionnaire de mots de passe est indispensable

Sécurité maximale

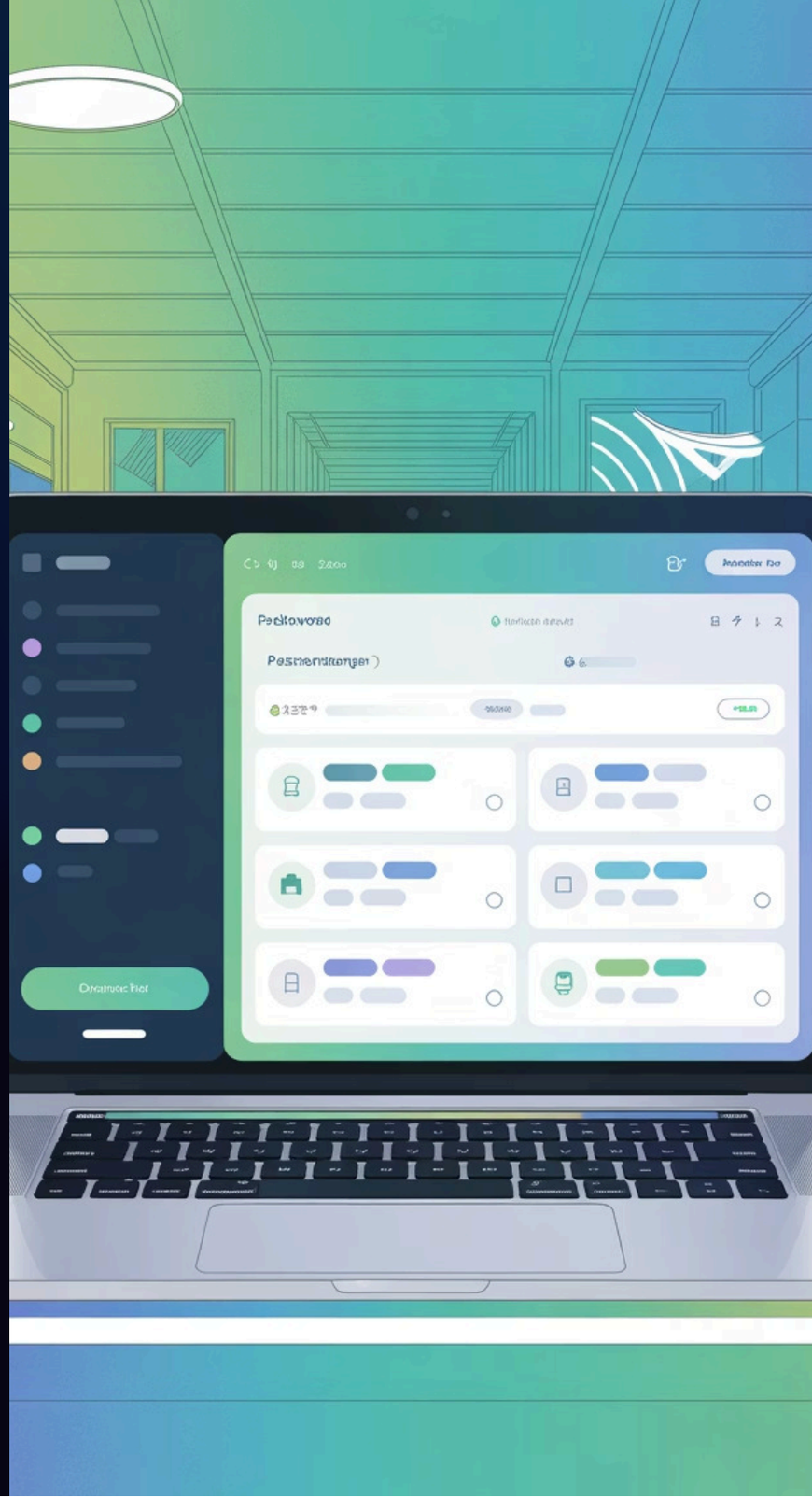
Il enregistre tous vos mots de passe de façon chiffrée et sécurisée, accessible uniquement par vous.

Fini les méthodes risquées

Il évite les blocs-notes, les fichiers Excel, les carnets papier et les post-it collés sur l'écran.

Création automatique

Il génère automatiquement des mots de passe complexes et impossibles à deviner pour chaque nouveau compte.



Authentification en deux étapes

La vraie protection supplémentaire

L'authentification à deux facteurs fonctionne comme une double clé pour votre porte.

Même si un mot de passe fuit ou est deviné, l'accès reste bloqué sans le second facteur de validation.

Ce second facteur peut être :

- Un code reçu par SMS
- Une notification sur votre téléphone
- Une application d'authentification
- Une clé de sécurité physique

Les erreurs les plus courantes

Noter sur papier

Les mots de passe écrits sur des post-it ou dans un carnet sont visibles par tous et facilement perdus.

Partager par mail

Les emails ne sont pas sécurisés. Un mot de passe envoyé par mail peut être intercepté ou retrouvé des années plus tard.

Garder le même partout

Utiliser un seul mot de passe pour tous vos comptes transforme une petite faille en catastrophe généralisée.

Mot de passe provisoire

Utiliser un mot de passe simple "en attendant" de le changer... et ne jamais le changer. C'est une porte ouverte permanente.

Sécuriser son entreprise en 30 jours

1

Semaine 1 : Inventaire

Faire la liste complète de tous les comptes professionnels : emails, banque, logiciels, réseaux sociaux, fournisseurs.

2

Semaine 2 : Équipement

Installer un gestionnaire de mots de passe professionnel pour toute l'équipe et former chacun à son utilisation.

3

Semaine 3 : Renouvellement

Modifier tous les mots de passe des comptes sensibles en utilisant le gestionnaire pour créer des mots de passe forts.

4

Semaine 4 : Double protection

Activer l'authentification à deux facteurs sur tous les comptes critiques : email, banque, administration.

Une politique interne simple à appliquer

Accès individuels

Chaque personne dispose de ses propres identifiants. Pas de compte partagé, même pour gagner du temps.

Zéro partage

Aucun mot de passe n'est communiqué, même entre collègues. Utilisez les fonctions de partage sécurisé si nécessaire.

Outil obligatoire

Tous les collaborateurs utilisent le gestionnaire de mots de passe fourni par l'entreprise, sans exception.

Renouvellement annuel

Les mots de passe des comptes les plus sensibles sont changés au moins une fois par an, ou immédiatement en cas de doute.

Ce que cela change concrètement

Dans une TPE/PME au quotidien

Moins de risques

Réduction drastique des risques de piratage et de blocage de l'activité.

Moins de stress

Tranquillité d'esprit sachant que vos données sont protégées efficacement.

Moins d'urgences

Fini les appels paniqués pour des comptes bloqués ou des accès perdus.

Plus de sécurité

Protection renforcée sans complexité technique ni formation compliquée.

Checklist prête à l'emploi

Gestionnaire installé ?

Ai-je un gestionnaire de mots de passe professionnel installé et configuré pour toute l'équipe ?

Double authentification active ?

Tous les comptes importants (email, banque, administration) ont-ils la double protection activée ?

Traces physiques éliminées ?

Y a-t-il encore des mots de passe notés sur papier, post-it, carnet ou fichier non sécurisé ?

Équipe sensibilisée ?

Les collaborateurs ont-ils été informés des bonnes pratiques et formés à l'utilisation des outils ?

Sécuriser les mots de passe n'est plus une option

C'est un geste simple qui évite des dégâts coûteux et protège l'avenir de votre entreprise.

Commencez dès aujourd'hui. Chaque jour sans protection est un jour de risque inutile.