LIVRE BLANC · ON PARLE SI ?

Mots de passe : la méthode qui protège vraiment

Longueur, phrase de passe, gestionnaire d'équipe, double authentification, clés d'accès — ce qui fonctionne réellement, et ce qui ne fonctionne plus.

Avant-propos

Pendant des années, la consigne a été la même partout : majuscule, chiffre, caractère spécial, changement tous les trois mois. Cette doctrine a produit exactement l'inverse de l'effet recherché — des mots de passe difficiles à retenir, donc réutilisés partout, notés sur un post-it, ou à peine modifiés d'un renouvellement à l'autre (« Ete2025! » devient « Ete2026! »).

Ce guide reprend le sujet à partir de ce qui protège réellement un compte aujourd'hui — la longueur avant la complexité, un gestionnaire plutôt qu'une mémoire humaine, une double vérification plutôt qu'un secret unique — et va jusqu'aux solutions qui commencent à remplacer le mot de passe lui-même.

1. Le vrai ennemi : la longueur, pas la complexité

Le facteur qui détermine le plus le temps nécessaire pour casser un mot de passe par force brute n'est pas la présence d'un caractère spécial — c'est le nombre de caractères. Chaque caractère supplémentaire multiplie le nombre de combinaisons possibles, alors qu'ajouter de la complexité sur un mot court n'apporte qu'un gain marginal.

MOT DE PASSE	TEMPS ESTIMÉ POUR LE CASSER
8 caractères, chiffres seuls	moins d'une seconde
8 caractères, alphanumérique + symboles	quelques heures à quelques jours
10 caractères, alphanumérique	quelques jours à deux semaines
12 caractères, alphanumérique + symboles	quelques mois à une dizaine d'années
15+ caractères, alphanumérique + symboles	des milliards d'années — hors de portée

Ces ordres de grandeur varient sensiblement d'une source à l'autre selon la puissance de calcul et l'algorithme de hachage supposés pour l'attaquant — ils ne doivent pas être lus comme des valeurs absolues.

Ce qui reste constant d'une estimation à l'autre, en revanche, c'est l'ordre de grandeur : un mot de passe de 8 caractères, même complexe, est aujourd'hui dans une zone de risque réaliste pour une entreprise ciblée, alors qu'à partir de 12-15 caractères on change complètement de catégorie de risque. La conclusion pratique est simple : viser la longueur d'abord, la complexité ensuite.

2. La méthode passphrase : un mot de passe long qu'on retient vraiment

Le principal obstacle à des mots de passe longs n'est pas technique, il est humain : personne ne mémorise naturellement 16 caractères aléatoires. La solution la plus robuste et la plus simple à adopter est la passphrase — une suite de mots ou une phrase personnelle, longue, mais facile à se remémorer parce qu'elle a un sens pour vous.

> **UN PIÈGE À ÉVITER**— NE JAMAIS CHOISIR UNE PHRASE DÉJÀ CONNUE — PAROLE DE CHANSON CÉLÈBRE, CITATION DE FILM, PROVERBE. C'EST PRÉCISÉMENT CE QUE LES ATTAQUANTS TESTENT EN PREMIER : DES LISTES ENTIÈRES DE PHRASES POPULAIRES EXISTENT POUR CE TYPE D'ATTAQUE, AVANT MÊME D'ESSAYER LES COMBINAISONS ALÉATOIRES.— EXEMPLE DE CONSTRUCTION CORRECTE, PERSONNELLE ET SANS SIGNIFICATION PUBLIQUE : UNE PHRASE INVENTÉE LIÉE À UN SOUVENIR PRÉCIS, PAR EXEMPLE « MONCHATATRAVERSELARUE3FOISENJUIN » — LONGUE, MÉMORISABLE, MAIS INTROUVABLE DANS AUCUNE LISTE.

Une passphrase de ce type dépasse facilement 20 caractères tout en restant plus facile à taper et à retenir qu'un mot de passe aléatoire de 12 caractères — et se situe, d'après le tableau précédent, largement au-delà de ce qui est cassable en pratique aujourd'hui.

3. Le gestionnaire de mots de passe : la seule solution qui tient à l'échelle d'une équipe

La méthode passphrase résout un mot de passe — celui qu'on retient. Elle ne résout pas le problème de fond d'une entreprise : des dizaines de comptes différents (outils SaaS, hébergement, banque en ligne, réseaux sociaux professionnels), chacun exigeant en théorie un mot de passe unique. Personne ne mémorise cinquante passphrases différentes.

Le gestionnaire de mots de passe règle ce problème une fois pour toutes : une seule passphrase forte protège un coffre-fort chiffré, qui génère et stocke un mot de passe unique et aléatoire pour chaque service. L'utilisateur ne retient plus qu'un seul secret ; le gestionnaire s'occupe du reste, y compris du remplissage automatique.

80% des violations de données impliquent un mot de passe compromis — la réutilisation d'un même mot de passe sur plusieurs services est le mécanisme le plus courant de propagation d'une fuite d'un site à l'autre (source : compilation sectorielle 2025-2026).

4. Grand public ou auto-hébergé : Vaultwarden, KeePass et les alternatives

Le choix du gestionnaire dépend moins des fonctionnalités — elles sont globalement comparables d'une solution à l'autre — que de qui héberge les données et qui porte la responsabilité de la sécurité de cet hébergement.

SOLUTION	OÙ SONT LES DONNÉES	CE QUE ÇA IMPLIQUE
SaaS grand public (Bitwarden, 1Password, Dashlane)	Chez l'éditeur, chiffrées	Le plus simple à mettre en place – abonnement mensuel par utilisateur, maintenance déléguée à l'éditeur
Vaultwarden (auto-hébergé, conteneur Docker)	Chez vous / votre hébergeur	Implémentation compatible Bitwarden, légère à déployer – licence gratuite, mais mises à jour et sauvegardes à votre charge
KeePass	Fichier local chiffré	Zéro dépendance cloud par défaut – la synchronisation entre appareils demande un mécanisme externe (Nextcloud, Syncthing…), moins pratique en équipe

Pour une petite structure sans compétence infra en interne, la solution SaaS reste le choix le plus rapide à mettre en œuvre. Pour une structure qui dispose déjà d'un hébergement maîtrisé – ou accompagnée sur ce point – un Vaultwarden auto-hébergé offre le même niveau de service sans coût de licence récurrent, au prix d'un peu de maintenance : c'est exactement le type de brique qui s'intègre à un audit et un pilotage infra plutôt qu'à un abonnement de plus à gérer soi-même.

---

5. La double authentification : le rempart contre 80% des violations

Un mot de passe, aussi long soit-il, reste un secret unique – s'il fuite (hameçonnage, fuite chez un fournisseur tiers), il tombe seul. La double authentification (MFA) ajoute une deuxième preuve d'identité, indépendante du mot de passe, qui neutralise la grande majorité des tentatives de connexion frauduleuses même en cas de mot de passe compromis.

- **Application d'authentification (TOTP)** – Google Authenticator, Aegis, Authy – génère un code à usage unique toutes les 30 secondes. Solution la plus simple à déployer, à privilégier par défaut.
- **SMS** – meilleur que rien, mais la moins robuste des trois options : vulnérable au détournement de numéro (SIM swap). À garder en solution de secours, pas en méthode principale.
- **Clé physique (type YubiKey)** – le niveau de protection le plus élevé, en particulier contre le hameçonnage. Pertinent pour les comptes les plus sensibles (accès admin, banque en ligne) plutôt que pour tous les usages du quotidien.

---

6. Le passwordless : deux approches, deux niveaux de maturité

Le lien magique par email

Un token de connexion unique envoyé par email, valable une seule fois – plus de mot de passe à retenir ni à gérer. C'est déjà le mode de connexion de nombreux outils SaaS courants. Simple à utiliser, mais cette simplicité déplace tout le risque sur un seul maillon : la boîte email elle-même. Si l'adresse email n'est pas elle-même protégée par une double authentification solide, cette méthode transforme la messagerie en clé maîtresse de tous les comptes qui en dépendent – une faiblesse, pas une protection.

Les passkeys (FIDO2)

Une approche plus aboutie techniquement : une paire de clés cryptographiques remplace le mot de passe, la clé privée ne quittant jamais l'appareil de l'utilisateur. Résistant par construction au hameçonnage, puisqu'il n'y a plus de secret à intercepter ou à saisir sur un faux site.

> **CE QUI EST DÉJÀ POSSIBLE AUJOURD'HUI**— MICROSOFT 365, GOOGLE WORKSPACE, ADOBE ET SALESFORCE SUPPORTENT NATIVEMENT LES PASSKEYS, TOUT COMME LES NAVIGATEURS MODERNES (CHROME, SAFARI, EDGE, FIREFOX).— DÉPLOIEMENT ESTIMÉ POUR UNE STRUCTURE DE 5 À 15 SALARIÉS : 500 À 1 500 € (AUDIT, CONFIGURATION, FORMATION), SUR 4 À 6 SEMAINES, AVEC COEXISTENCE INITIALE DES MOTS DE PASSE EXISTANTS PENDANT LA TRANSITION.

---

7. Quelle solution pour quelle TPE-PME

- **Petite structure, budget serré** – gestionnaire de mots de passe SaaS + application TOTP pour la double authentification. C'est le socle minimal qui couvre l'essentiel du risque pour quelques euros par mois et par utilisateur.
- **Structure avec un accompagnement infra (audit, hébergement déjà suivi)** – Vaultwarden auto-hébergé plutôt qu'un abonnement récurrent – même service, coût de licence nul, maintenance intégrée à ce qui est déjà suivi par ailleurs.
- **Structure déjà sur Microsoft 365 ou Google Workspace, prête à moderniser** – passkeys : le support natif existe déjà, il ne reste qu'à l'activer et accompagner la transition.
- **Lien magique par email** – pratique pour des outils annexes à faible enjeu, jamais comme unique protection d'un compte sensible sans que la messagerie elle-même soit verrouillée au maximum en amont.

Conclusion

La hiérarchie est claire : la longueur protège plus que la complexité, un gestionnaire de mots de passe protège plus qu'une mémoire humaine aussi disciplinée soit-elle, et la double authentification neutralise la plupart des compromissions même quand un mot de passe finit par fuiter. Le passwordless – passkeys en tête – est la direction vers laquelle tout le monde va, mais un gestionnaire de mots de passe bien utilisé, associé à une double authentification systématique, reste aujourd'hui le socle réaliste pour la quasi-totalité des TPE-PME.

Aucune de ces mesures ne demande un investissement technique lourd. Elles demandent une décision et, pour certaines, une heure d'accompagnement pour bien démarrer – ce qui en fait sans doute le rapport protection / effort le plus favorable de toute la sécurité informatique d'une PME.

À propos

Ce guide est publié par **l'association « On parle SI ? »**, qui explique l'informatique d'entreprise aux dirigeants de TPE et de PME – en vidéo, en conférence et dans des documents comme celui-ci.

L'association ne commercialise aucun produit ni aucune prestation. Ce document est diffusé librement, sans formulaire et sans contrepartie, et il est écrit pour rester utile même si vous ne faites appel à personne pour vous accompagner.

Ses membres exercent par ailleurs une activité professionnelle dans le secteur informatique, au sein de structures distinctes qui n'interviennent ni dans la ligne éditoriale, ni dans le financement de ces publications.

Les ordres de grandeur cités proviennent de sources publiques ou de plusieurs acteurs du secteur et sont donnés à titre indicatif. Une erreur, une question, une remarque : contact@onparlesi.fr.
