

Bien gérer ses mots de passe : le système qui tient

Catégorie : L'Art de s'organiser · Mots-clés : gérer ses mots de passe entrepreneur, organisation numérique

La plupart des entrepreneurs que j'accompagne gèrent leurs mots de passe de la même façon : en improvisant. Un fichier texte ouvert quelque part, quelques variantes d'un même mot de passe, des Post-it perdus dans un tiroir. Le tout fonctionne jusqu'au jour où ça ne fonctionne plus.

Ce n'est pas une question de négligence. C'est une question de système. Et un système, ça se construit.

Un mot de passe par compte, sans exception

C'est la base qui change tout. Quand tu utilises le même mot de passe sur plusieurs services et que l'un d'eux est compromis, tous tes comptes le sont. Ce n'est pas une probabilité abstraite — c'est ce qui arrive quotidiennement à des entrepreneurs qui n'avaient rien fait de particulièrement imprudent.

Un mot de passe unique par compte, c'est la première décision structurante. Tout le reste s'organise autour.

Ce qui fait un mot de passe robuste

Longueur d'abord. Seize caractères valent mieux que huit, quelle que soit leur complexité apparente. Mélange ensuite : majuscules, minuscules, chiffres, symboles. Pas de mots reconnaissables, pas de dates personnelles, pas de prénoms.

Une phrase transformée fonctionne bien : "Mon premier client en 2016" devient "M0nPr3mierCl!ent2016". Mémorisable pour toi, illisible pour un système automatique.

Quand changer ses mots de passe

Pas besoin de le faire tous les mois. Cette habitude conduit généralement à choisir des mots de passe de plus en plus faibles pour tenir le rythme. Change un mot de passe dans deux situations précises : quand le service concerné signale une fuite de données, et tous les six à douze mois sur tes comptes les plus sensibles.

Le site Have I Been Pwned (haveibeenpwned.com) te permet de vérifier si ton adresse email est apparue dans une fuite connue. Une vérification rapide, utile à faire de temps en temps.

La double authentification sur les comptes critiques

Sur ta messagerie principale, ta banque et tes espaces clients sensibles, active la double authentification. Même mot de passe volé, accès impossible sans le second code. C'est la mesure qui change réellement la donne sur les comptes qui comptent vraiment.

Le stockage : papier, numérique, ou les deux

Un mot de passe unique par compte, ça suppose de le conserver quelque part. Deux approches fonctionnent : un gestionnaire numérique dédié, synchronisé entre tes appareils, ou un carnet organisé de A à Z, consultable à tout moment sans dépendre d'un service tiers.

Les deux ont leurs avantages. Le numérique est plus rapide au quotidien. Le papier est inviolable à distance et ne dépend d'aucun cloud. Beaucoup d'entrepreneurs utilisent les deux en complément.

Le meilleur système est celui que tu utilises vraiment. Commence par tes dix comptes les plus utilisés. Génère des mots de passe uniques pour chacun. Stocke-les dans le format qui correspond à ton fonctionnement. Ensuite seulement, élargis progressivement.

Outils, méthodes et ressources pour organiser tes mots de passe au quotidien.

[Voir les ressources](#)