Une clé différente pour chaque porte

Démonstration imprimée de la réutilisation. Les clés A à E sont fictives : elles ne représentent aucun vrai mot de passe.

Le passe-partout

Lorsqu'une même clé protège plusieurs services, une fuite sur le compte le moins important peut fournir l'accès à l'e-mail, aux achats ou aux réseaux sociaux.

> La longueur ne corrige pas la réutilisation. Une très longue clé réutilisée reste un lien entre toutes les portes.

La séparation

Avec une clé indépendante par service, la fuite d'un compte de loisirs ne donne pas automatiquement la clé de la messagerie ou de la banque.



Même clé réutilisée	E-mail	Banque	Documents	Achats	Loisirs
Après la fuite de Loisirs	CLÉ A	CLÉ A	CLÉ A	CLÉ A	CLÉ A
Clés indépendantes	CLÉ A	CLÉ B	CLÉ C	CLÉ D	CLÉ E

Dans quel ordre changer ?

Commencez par les comptes qui récupèrent, paient ou prouvent votre identité. Avancez ensuite par petits lots.

1 E-mail principal

Il reçoit souvent les liens de récupération des autres comptes.

Action : Vérifier récupération, sessions et deuxième facteur.

2 Argent et identité

Banque, paiement, impôts, santé et démarches administratives.

Action : Changer les secrets réutilisés depuis les accès officiels.

3 Documents et communications

Stockage, photos, messageries et comptes liés au téléphone.

Action : Contrôler les appareils, transferts et méthodes de secours.

4 Achats et réseaux sociaux

Boutiques, livraison, plateformes de vente et réseaux sociaux.

Action : Retirer les cartes inutiles et fermer les sessions inconnues.

5 Loisirs et abonnements

Jeux, vidéo, musique, forums et services secondaires.

Action : Traiter par lots de trois à cinq comptes.

6 Anciens comptes

Services oubliés, essais gratuits et comptes jamais utilisés.

Action : Supprimer lorsque la procédure est claire et les données récupérées.

Ne changez pas un mot de passe uniquement parce qu'une date est passée. Traitez d'abord les secrets réutilisés, suspects ou concernés par une fuite, puis les comptes prioritaires.

Si vous suspectez un appareil infecté, utilisez un appareil sain pour sécuriser d'abord l'e-mail principal.

Ordre de changement imprimable

Inscrivez seulement le nom du service et l'état des contrôles. Ne notez jamais le mot de passe, un code bancaire ou un code de récupération.

Service	Priorité 1 à 6	Réutilisé ?	Récupération vérifiée	Secret unique	Deuxième preuve	Sessions contrôlées	Date
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	
		Oui / Non	☐	☐	☐	☐	

Ma première session de 15 minutes

Objectif : casser une seule réutilisation importante aujourd'hui, puis préparer le prochain lot.

Avant de commencer

- ☐ J'utilise un appareil sain et à jour.
- ☐ J'ouvre chaque service moi-même, sans suivre le lien d'une alerte.
- ☐ Je vérifie la récupération avant de fermer la session courante.
- ☐ Mon gestionnaire de mots de passe est prêt ou ma méthode sûre est définie.
- ☐ Je prévois des lots courts plutôt qu'un changement précipité de tous les comptes.

Compte traité aujourd'hui

Service _____

Catégorie de priorité _____

Date _____

Contrôles terminés

- ☐ Le mot de passe est réellement unique, pas une variante.
- ☐ La récupération est actuelle et testable.
- ☐ Le deuxième facteur est activé lorsqu'il est proposé.
- ☐ Les sessions et appareils inconnus sont déconnectés.
- ☐ Le prochain lot de trois à cinq comptes est noté.

Prochain lot

Compte 1 _____

Compte 2 _____

Compte 3 _____

Ressources officielles

CNIL - Exposition d'identifiants et mots de passe : que faire ? - cnil.fr - Exposition d'identifiants

Cybermalveillance.gouv.fr - Comment choisir un bon mot de passe ? - cybermalveillance.gouv.fr - Bon mot de passe

CNIL - Authentification par mot de passe - cnil.fr - Mesures de sécurité élémentaires

Liens vérifiés le 23 juillet 2026.