Une deuxième serrure que vous pourrez garder

Comparatif maintenu et vérifié le 23 juillet 2026. La meilleure méthode est la plus robuste que vous pouvez utiliser et récupérer sans improviser.

1. Protégez d'abord

E-mail principal, gestionnaire de mots de passe, argent, identité, stockage et communications.

2. Choisissez durablement

Préférez une méthode résistante au hameçonnage lorsqu'elle est disponible. Sinon, activez la meilleure option proposée.

3. Préparez la sortie

Enregistrez un secours distinct avant de retirer l'ancienne méthode ou de changer de téléphone.

Compte critique

E-mail, gestionnaire, banque, identité ou compte système.

- ☐ Clé d'accès si le service et vos appareils la prennent bien en charge.
- ☐ Clé physique avec un double enregistré.
- ☐ Application de codes si les options précédentes ne conviennent pas.
- ☐ SMS si c'est la seule méthode disponible : activez-le quand même.

Contraintes réelles

- ☐ Réseau mobile parfois absent.
- ☐ Plusieurs systèmes ou appareils.
- ☐ Téléphone souvent remplacé ou partagé.
- ☐ Risque de perte de la clé physique.
- ☐ Besoin d'aide d'une personne de confiance.

Une contrainte ne signifie pas « aucune MFA ». Elle indique le secours à préparer et la méthode à tester avant migration.

Validation inattendue : si vous n'avez commencé aucune connexion, refusez ou fermez. Des demandes répétées peuvent indiquer que le mot de passe est déjà connu : ouvrez le service par votre chemin habituel, changez le secret et contrôlez les sessions.

Ma méthode principale

Compte _____

Méthode _____

Ma récupération

Secours _____

Lieu général _____

Comparatif des seconds facteurs

La résistance au hameçonnage est relative : elle décrit la capacité de la méthode à éviter qu'une preuve soit utilisée sur un faux service. Elle ne garantit jamais un risque nul.

Méthode	Hameçonnage	Réseau	Si l'appareil disparaît	Secours à préparer	Usage conseillé
Code par SMS Mieux qu'un mot de passe seul, mais le code peut être dicté, intercepté ou visé par un transfert frauduleux du numéro.	**Faible**	Réseau mobile requis	Dépend du numéro et de l'opérateur	Méthode secondaire distincte	À activer si c'est la seule option
Application de codes Le code temporaire peut encore être copié dans un faux site ou dicté à un fraudeur. Préparez le changement de téléphone.	**Limitée**	Souvent inutile pour générer le code	Transfert ou sauvegarde à préparer	Codes de secours ou autre appareil	Bonne option courante
Notification d'approbation Lisez le service, l'action et le contexte. Des demandes répétées peuvent chercher une validation par fatigue.	**Variable**	Connexion nécessaire	Autre appareil ou méthode requise	Code de secours ou méthode secondaire	Simple si la demande est contextualisée
Clé de sécurité physique Une clé compatible vérifie le service auquel elle répond. Enregistrez un double avant de dépendre de la première.	**Élevée**	Pas de réseau mobile requis	Prévoir un double	Deuxième clé ou méthode officielle	Comptes critiques et personnes ciblées
Clé d'accès ou passkey La preuve cryptographique est liée au vrai service. Vérifiez comment elle suit vos appareils et comment le compte se récupère.	**Élevée**	Selon le service et la synchronisation	Dépend des appareils et de la synchronisation	Autre appareil ou récupération du compte	À privilégier lorsqu'elle est bien prise en charge

Codes de récupération : ils ne sont pas un second facteur quotidien. Ce sont des clés de secours, souvent à usage unique, capables de contourner l'indisponibilité de la méthode principale.

Biométrie : visage ou empreinte déverrouillent souvent une preuve conservée par l'appareil. La solidité dépend aussi du code local, de l'appareil et de la méthode sous-jacente.

Récupération fictive : téléphone principal perdu

Exercice sans compte réel. Aucun code n'est affiché. Le but est de suivre l'ordre des décisions, pas de mémoriser une procédure universelle.

Situation

Compte : julien@exemple.invalid

Perdu : téléphone principal utilisé pour les validations

Disponible : ordinateur déjà reconnu, enveloppe papier avec un code fictif masqué, nouveau téléphone non configuré

Un SMS urgent affirme : « Votre compte sera fermé. Récupérez-le ici. » Le lien ne fait pas partie de l'exercice sûr.

Objectif

Retrouver l'accès depuis un canal déjà connu, retirer l'appareil perdu, ajouter un nouveau facteur et renouveler les secours potentiellement exposés.

Règles

- ☐ Ne suivre aucun lien reçu pendant l'incident.
- ☐ Ne dicter aucun code à un support.
- ☐ Ne supprimer l'ancienne méthode qu'après un accès confirmé.
- ☐ Conserver les preuves si une session inconnue apparaît.

1. Entrer

Utiliser l'ordinateur reconnu ou saisir soi-même l'adresse officielle.

2. Prouver

Choisir le code de secours fictif masqué ou une autre méthode déjà enregistrée.

3. Nettoyer

Retirer le téléphone perdu et fermer les sessions inconnues.

4. Reconstruire

Ajouter le nouveau téléphone, tester, puis renouveler les secours.

Journal de l'exercice

Canal utilisé _____

Preuve choisie _____

Appareil retiré _____

Nouveau test _____

Fin de récupération

- ☐ L'accès est confirmé avant toute suppression.
- ☐ Le téléphone perdu est retiré.
- ☐ Les sessions inconnues sont fermées.
- ☐ Le nouveau facteur fonctionne.
- ☐ Les codes de secours sont renouvelés si nécessaire.

Si aucune méthode sûre ne fonctionne : arrêtez les essais répétés et utilisez uniquement la récupération officielle du service. Les délais et preuves demandées varient ; un support légitime ne vous demande pas de lui dicter un code de connexion.

Liens officiels et maintenance

Répertoire non exhaustif. Liens contrôlés le 23 juillet 2026. Les fonctions des services évoluent : vérifiez toujours la page officielle avant de modifier vos facteurs.

Repères publics

CNIL - Recommandation sur l'authentification multifacteur

Recommandation adoptée en mars 2025.

Repères publics

CNIL - Utiliser la MFA pour les comptes en ligne

Présentation destinée aux utilisateurs.

Repères publics

ANSSI - MFA et mots de passe

Guide technique officiel et analyse du contexte.

Repères publics

Cybermalveillance.gouv.fr - Double authentification

Article mis à jour le 25 février 2026.

Réaction

Cybermalveillance.gouv.fr - Compte piraté

Fiche réflexe mise à jour le 7 mai 2026.

Standard

FIDO Alliance - Passkeys

Présentation du standard et de sa résistance au hameçonnage.

Exemple de récupération

Google - Validation en deux étapes

Méthodes, clés et codes de secours.

Exemple de récupération

Microsoft - Vérification en deux étapes

Configuration et informations de récupération.

Exemple de récupération

Mozilla - Authentification à deux facteurs

Configuration et codes de secours.

Contrôle trimestriel

- ☐ Les appareils reconnus sont encore possédés.
- ☐ La méthode secondaire fonctionne.
- ☐ Les secours sont lisibles et protégés.
- ☐ Les coordonnées de récupération sont à jour.

À partager en famille

Chacun doit savoir reconnaître une demande inattendue et retrouver son propre secours. N'accumulez pas tous les facteurs sur le téléphone d'une seule personne.

Prochain test _____

Personne aidée _____