Sécurisez votre ordinateur, sans l'alourdir

Parcours Windows et macOS vérifiés le 23 juillet 2026. Le but est de contrôler les protections déjà présentes, leur récupération et les sessions, sans installer un nouvel outil par réflexe.

1. Ouvrir depuis le système

Une vraie protection intégrée s'ouvre depuis les Paramètres ou Réglages Système, pas depuis une page web.

2. Vérifier avant de modifier

Lisez l'état du chiffrement et retrouvez le chemin de récupération avant toute activation ou désactivation.

3. Séparer les usages

Une session par utilisateur régulier, peu d'administrateurs et un verrouillage dès que l'écran est laissé seul.

Avant d'ouvrir les réglages

- ☐ Je connais la version du système et le propriétaire de l'ordinateur.
- ☐ Je dispose d'une sauvegarde avant une modification importante.
- ☐ Je sais quel compte est administrateur.
- ☐ Je n'inscris aucun mot de passe ni aucune clé sur cette fiche.
- ☐ Je peux consulter une aide officielle depuis un autre appareil.

Mes repères sans secret

Ordinateur ou propriétaire _____

Système et version _____

Administrateur, nom abrégé _____

Lieu général de récupération _____

Date du prochain contrôle _____

Fausse alerte de support

Une page qui bloque le navigateur et demande d'appeler un numéro n'est pas Sécurité Windows ni une alerte normale de macOS. N'appelez pas, n'installez rien et n'autorisez aucune prise en main.

Parcours Windows

Chemins contrôlés le 23 juillet 2026 pour Windows 11 et, lorsque Microsoft l'indique encore, Windows 10. Les intitulés peuvent varier selon l'édition et la gestion de l'appareil.

1. Installer les mises à jour

Chemin courant : Démarrer > Paramètres > Windows Update

Recherchez les mises à jour, installez-les puis redémarrez si Windows le demande. Sauvegardez avant une évolution importante.

Test sans risque : L'état indique que l'appareil est à jour ou précise clairement ce qui reste à installer.

Microsoft Support - Installer les mises à jour Windows

2. Verrouiller la session

Chemin courant : Paramètres > Comptes > Options de connexion

Vérifiez la méthode de connexion et les options supplémentaires. Utilisez Windows + L dès que vous quittez l'écran.

Test sans risque : Verrouillez avec Windows + L, puis reconnectez-vous sans laisser une autre personne regarder le code.

Microsoft Support - Options de connexion

3. Séparer les utilisateurs

Chemin courant : Paramètres > Comptes > Autres utilisateurs

Créez un compte par utilisateur régulier. Limitez les administrateurs et préférez un compte standard pour l'usage quotidien.

Test sans risque : Chaque personne retrouve ses propres documents et connexions sans utiliser la session d'un proche.

Microsoft Support - Gérer les comptes utilisateur

4. Ouvrir Sécurité Windows

Chemin courant : Démarrer > Sécurité Windows > Protection contre les virus et menaces

Lisez l'état affiché et lancez une analyse rapide si vous souhaitez contrôler le socle. Une analyse hors connexion redémarre le PC.

Test sans risque : L'historique et les actions recommandées sont consultés depuis l'application, jamais depuis une alerte web.

Microsoft Support - Protection contre les virus et menaces

5. Vérifier le pare-feu

Chemin courant : Sécurité Windows > Pare-feu et protection réseau

Contrôlez que le pare-feu est actif pour le profil utilisé. Autorisez une application précise plutôt que de désactiver toute la protection.

Test sans risque : Le profil réseau actuel affiche le pare-feu actif et aucune désactivation générale n'est laissée en place.

Microsoft Support - Pare-feu et protection réseau

6. Contrôler le chiffrement

Chemin courant : Paramètres > Confidentialité et sécurité > Chiffrement de l'appareil

L'option dépend du matériel, de l'édition et du compte. Avant toute modification, identifiez l'endroit où se trouve la clé BitLocker.

Test sans risque : Vous connaissez l'état du chiffrement et le lieu de récupération, sans afficher ni recopier la clé sur cette fiche.

Microsoft Support - Chiffrement de l'appareil

Repère daté : Microsoft indique que le support gratuit de Windows 10 a pris fin le 14 octobre 2025. Un PC encore sous Windows 10 demande donc un plan de mise à niveau ou de remplacement compatible.

Parcours macOS

Chemins contrôlés le 23 juillet 2026. Apple n'affiche que les mises à jour compatibles avec le modèle ; les réglages peuvent varier sur une ancienne version de macOS.

1. Installer les mises à jour

Chemin courant : Menu Pomme > Réglages Système > Général > Mise à jour logicielle

Installez la dernière version compatible proposée par le Mac. Sauvegardez avant une évolution importante.

Test sans risque : Mise à jour logicielle indique que le Mac est à jour ou précise clairement l'installation restante.

Apple Support - Mettre à jour macOS

2. Verrouiller la session

Chemin courant : Menu Pomme > Réglages Système > Écran verrouillé

Exigez un mot de passe après l'extinction de l'écran. Utilisez le menu Pomme > Verrouiller l'écran quand vous vous éloignez.

Test sans risque : Verrouillez, puis reconnectez-vous sans laisser une autre personne regarder le mot de passe.

Apple Support - Réglages Écran verrouillé

3. Séparer les utilisateurs

Chemin courant : Menu Pomme > Réglages Système > Utilisateurs et groupes

Créez un compte par utilisateur régulier. Limitez les administrateurs et utilisez un compte standard lorsque cela convient.

Test sans risque : Chaque personne retrouve ses propres documents et connexions sans utiliser la session d'un proche.

Apple Support - Ajouter un utilisateur

4. Garder la protection intégrée

Chemin courant : Réglages Système > Confidentialité et sécurité > Sécurité

Conservez les contrôles des applications. Ne passez pas outre une alerte pour un logiciel inattendu ou d'origine inconnue.

Test sans risque : Les applications autorisées viennent de l'App Store ou de développeurs connus, selon votre choix.

Apple Support - Protéger le Mac contre les logiciels malveillants

5. Vérifier le coupe-feu

Chemin courant : Réglages Système > Réseau > Coupe-feu

Contrôlez qu'il est actif. Avant d'ajouter une exception, vérifiez l'application et les services de partage réellement nécessaires.

Test sans risque : Le coupe-feu est actif et aucune ouverture temporaire oubliée n'apparaît dans les options.

Apple Support - Réglages Coupe-feu

6. Contrôler FileVault

Chemin courant : Réglages Système > Confidentialité et sécurité > FileVault

Lisez l'état sans modifier. Avant toute activation, identifiez le chemin choisi : compte Apple, clé de secours ou gestion de l'organisation.

Test sans risque : Vous connaissez l'état de FileVault et le lieu de récupération, sans afficher ni recopier la clé sur cette fiche.

Apple Support - Protéger les données avec FileVault

Repère matériel : Apple indique que les Mac à puce Apple ou avec puce T2 chiffrent déjà les données. FileVault ajoute la protection liée au mot de passe de session et au chemin de récupération choisi.

Clé de récupération et sessions

Ne testez jamais la récupération en provoquant volontairement un verrouillage. Vérifiez seulement l'état, le lieu général et l'accès au compte ou au support responsable.

Windows - BitLocker

La clé de récupération est un nombre de 48 chiffres. Microsoft indique ne pas pouvoir la recréer si elle est perdue.

Emplacements possibles : compte Microsoft, compte professionnel ou scolaire, impression, clé USB ou responsable informatique.

- ☐ Je connais l'état du chiffrement.
- ☐ Je sais quel compte ou responsable détient la récupération.
- ☐ Je peux ouvrir le lieu de récupération depuis un autre appareil.
- ☐ La clé n'est pas conservée seulement sur le disque chiffré.

Microsoft Support - Rechercher la clé BitLocker

Compte Microsoft - Mes clés de récupération

macOS - FileVault

Le chemin peut utiliser le compte Apple, une clé de secours personnelle ou la gestion d'une organisation. Apple avertit qu'une récupération perdue peut rendre les fichiers inaccessibles.

À conserver : une clé personnelle doit être exacte, protégée et rangée ailleurs que sur le Mac concerné.

- ☐ Je connais l'état de FileVault.
- ☐ Je sais si la récupération utilise le compte Apple, une clé ou l'organisation.
- ☐ La clé personnelle éventuelle est rangée hors du Mac.
- ☐ Les utilisateurs autorisés à déverrouiller le disque sont identifiés.

Apple Support - FileVault et clé de secours

Sessions Windows

- ☐ Chaque utilisateur régulier dispose de sa propre session.
- ☐ Le nombre d'administrateurs est limité et compris.
- ☐ L'ouverture automatique n'expose pas une session sensible.
- ☐ Le verrouillage est utilisé dès que l'écran est laissé seul.

Sessions macOS

- ☐ Chaque utilisateur régulier dispose de sa propre session.
- ☐ Le nombre d'administrateurs est limité et compris.
- ☐ L'ouverture automatique n'expose pas une session sensible.
- ☐ Le verrouillage est utilisé dès que l'écran est laissé seul.

Liens officiels et contrôle trimestriel

Répertoire contrôlé le 23 juillet 2026. Les pages officielles restent la référence lorsque les menus, éditions, matériels ou politiques d'organisation évoluent.

Microsoft Support

Mises à jour

Microsoft Support - Installer les mises à jour Windows

Connexion et verrouillage

Microsoft Support - Options de connexion

Sessions et administrateurs

Microsoft Support - Gérer les comptes utilisateur

Sécurité intégrée

Microsoft Support - Protection contre les virus et menaces

Pare-feu

Microsoft Support - Pare-feu et protection réseau

Chiffrement

Microsoft Support - Chiffrement de l'appareil

Clé BitLocker

Microsoft Support - Rechercher la clé de récupération BitLocker

Apple Support

Mises à jour

Apple Support - Mettre à jour macOS

Écran verrouillé

Apple Support - Réglages Écran verrouillé

Sessions et administrateurs

Apple Support - Ajouter un utilisateur

Protection intégrée

Apple Support - Protéger le Mac contre les logiciels malveillants

Coupe-feu

Apple Support - Réglages Coupe-feu

FileVault et récupération

Apple Support - Protéger les données avec FileVault

Contrôle trimestriel

- ☐ Le système et les protections intégrées sont à jour.
- ☐ Le pare-feu ou coupe-feu est actif.
- ☐ Le chiffrement et son chemin de récupération sont connus.
- ☐ Les sessions et droits d'administration restent cohérents.

Règle familiale

Une alerte qui demande d'appeler n'est pas appelée. Nous fermons le navigateur, puis nous ouvrons la sécurité depuis le système. Aucun code et aucune prise en main ne sont accordés sous pression.

Prochain contrôle _____

Personne accompagnée _____