



FICHE PRATIQUE

Mettre à jour ses appareils

80 % des cyberattaques exploitent une faille déjà corrigée. Ne soyez pas victime d'un correctif oublié.

Pourquoi c'est critique

- Chaque mise à jour comble des failles découvertes depuis la précédente.
- Les attaquants scannent en permanence Internet à la recherche d'appareils non à jour.
- Un appareil non patché reste vulnérable **indéfiniment**.

Ce qu'il faut mettre à jour

- **Système d'exploitation** : Windows, macOS, iOS, Android, Linux.
- **Navigateurs** : Chrome, Firefox, Edge, Safari.
- **Applications** : suite bureautique, lecteur PDF, messageries.
- **Box internet et routeurs** : firmware.
- **Objets connectés** : caméras, imprimantes, NAS, enceintes.

Activer la mise à jour automatique

- Windows : Paramètres > Windows Update > Options avancées.
- macOS : Réglages Système > Général > Mise à jour de logiciels.
- iOS / Android : activer les MAJ auto dans les paramètres système et store.
- Box : la plupart des FAI font ces MAJ automatiquement, vérifiez quand même.

Fin de support : le piège

- Windows 10 : fin du support en octobre 2025 migrer vers Windows 11 ou Linux.
- Smartphones : 2 à 5 ans de MAJ selon les marques. Au-delà, à remplacer.
- Objets connectés : vérifiez la durée de support promise par le fabricant.

Pour les pros

- Tenez un **inventaire** de vos appareils, OS et logiciels.
- Définissez une **fenêtre de maintenance** mensuelle.
- Pour les serveurs : testez les MAJ sur un environnement de pré-production.

Patch management externalisé ?

BigFamily supervise les mises à jour de votre parc, sans interrompre votre activité.