



FICHE PRATIQUE

Sécurité sur les réseaux sociaux

Profiter des réseaux sans en payer le prix fort en données ou en réputation.

Réglages de confidentialité

- Profil privé par défaut sur Instagram, Facebook, TikTok, X.
- Listes d'amis et abonnements **cachés**.
- Géolocalisation désactivée pour les photos.
- Visibilité du téléphone et de l'email : amis uniquement, ou personne.

Ce qu'on ne publie pas

- Photos d'enfants identifiables (école, prénom + nom).
- Plaque d'immatriculation, carte d'embarquement, billets de spectacle.
- Vacances en temps réel (signal qu'il n'y a personne à la maison).
- Informations professionnelles confidentielles, organigrammes.

Sécurité du compte

- Mot de passe unique et long.
- **Double authentification** activée (appli plutôt que SMS).
- Vérifiez régulièrement les **sessions actives** et les applis tierces autorisées.
- Email de récupération sécurisé.

Reconnaître les arnaques

- Faux profils qui tentent de devenir « ami » pour collecter des infos.
- Faux jeux concours, faux SAV de marque, faux livreurs.
- Investissements en crypto ou en trading « miraculeux ».

Pour les pros

- Comptes pro et perso bien séparés.
- Sur LinkedIn : attention aux fausses demandes de recruteurs (collecte d'infos).

Ateliers pour ados ou seniors ?

BigFamily Académie intervient aussi en milieu scolaire, associatif, et en entreprise.