

Les réflexes indispensables pour installer des applications IPA en toute sécurité

Sources et installation sécurisée

- Privilégiez systématiquement l'App Store officiel, qui applique des processus de revue de sécurité stricts pour prévenir les malwares.
- Si vous utilisez le sideloading dans l'UE, vérifiez que l'App Marketplace dispose d'une autorisation Apple valide.
- Pour les fichiers .ipa issus de la distribution d'entreprise, vérifiez manuellement le certificat dans 'Réglages > Général > Gestion des appareils'.

Configuration et protection du système

- Désactivez le 'Mode développeur' dans 'Réglages > Confidentialité et sécurité' lorsqu'il n'est pas activement utilisé pour limiter la surface d'attaque.
- Ne faites jamais confiance aux profils de configuration (MDM) provenant de sources tierces inconnues, car ils peuvent offrir un accès total à vos données.
- Évitez le jailbreak de votre iPhone, qui désactive les protections essentielles du noyau (kernel) et expose vos données privées.

Surveillance et gestion des permissions

- Examinez les permissions accordées à chaque application dans 'Réglages > [Nom de l'app]' et révoquez l'accès au micro, aux contacts ou à la localisation si non indispensable.
- Utilisez le 'Rapport de confidentialité de l'app' dans 'Réglages > Confidentialité et sécurité' pour surveiller les domaines internet contactés par vos applications.
- Ne partagez jamais vos identifiants Apple ou mots de passe avec des services tiers promettant des applications 'premium' gratuites via des fichiers IPA modifiés.