# Avertissements

L’utilisation d’une tablette Android implique la connexion à un compte Google.
Ce compte Google, associé à la tablette, est utilisé par certaines applications. Decalog déconseille de ce fait d'autoriser l'accès à ces applications, d'autant plus qu’il est possible de lier un moyen de paiement au compte Google via le service Google Wallet. L’utilisation par l’usager d’applications tirant partie de ce dispositif pourrait entraîner des coûts importants à la bibliothèque.
*Par exemple, le navigateur Google Chrome pourrait permettre aux usagers de s’identifier sur tous les services Google tels que Gmail ou Drive avec le compte Google lié à la tablette et ainsi envoyer des mails en usurpant l’identité de la bibliothèque.*

L’un des principes de base de la sécurité sous Android est qu’une application non identifiée comme " application système" ne peut interférer avec les données d’une autre application. De plus, une " application système" ne peut être qu’une application développée par Google ou par le constructeur de la tablette, ce qui signifie que le client EPN développé par Decalog n’en fait pas partie.
Par conséquent, dans le cas où des fichiers sont créés localement sur la tablette par une des applications autorisées, ils ne peuvent pas être supprimés à la fermeture de la session utilisateur.
*Un cas concret : si une application de traitement de texte est rendue accessible aux usagers, tous les fichiers textes créés par celle-ci resteront disponibles d’une session à l’autre.*

Il n’est pas non plus possible de restreindre l’accès aux paramètres d’une application à partir du moment où cette application est autorisée.
*Par exemple, si un usager modifie les paramètres linguistiques d’une application autorisée, le prochain usager qui lancera cette même application utilisera ce même paramétrage.*

Il faut toujours garder en tête que les tablettes Android sont censées être à la base des périphériques personnels, par conséquent toutes les applications disponibles ne sont pas forcément adaptées à un usage dans un espace public numérique.

> De manière générale, Decalog recommande donc de tester chaque nouvelle application à autoriser afin de vérifier son bon fonctionnement mais aussi de s’assurer que les contraintes citées ci-dessus n’entrainent pas une faille de sécurité.

---

Created 2026-10-03 13:52:34 UTC by Admin
Updated 2026-10-03 13:52:51 UTC by Admin