

04.09.2025

Surveiller les autorisations d'application pour garder le contrôle sur vos données

Lors de l'installation, de nombreuses applis demandent plus d'autorisations que nécessaire. En limitant et en vérifiant régulièrement les différentes autorisations accordées aux applications, non seulement vous contribuez à protéger votre vie privée, mais vous empêchez aussi que vos données personnelles ne soient siphonnées à votre insu.

Qu'il s'agisse de filtres photo, de jeux ou de réseaux sociaux, beaucoup d'applications exigent des autorisations d'accès à des fonctions et à des données de votre smartphone. Ces autorisations sont justifiées lorsque l'accès est techniquement nécessaire, comme dans le cas d'un éditeur de photos qui demande l'autorisation d'accéder à la galerie de photos, ou pour une application de navigation qui a besoin d'accéder aux données de géolocalisation. Or il n'est pas rare que les applis demandent des droits d'accès plus étendus, comme si une application de lampe de poche avait besoin d'accéder à vos contacts. Ce type d'abus peut présenter des risques.

Voici ce que vous pouvez faire :

Android

- **Adapter constamment les droits d'accès:** dans les paramètres (Sécurité & Confidentialité > Paramètres de confidentialité > Gestionnaire d'autorisations) vous avez la possibilité d'activer ou de révoquer les autorisations aux applis de votre choix.
- **Limitier les droits d'accès:** depuis Android 11, les accès sensibles, comme pour l'appareil photo, le micro ou la localisation peuvent être accordés de manière temporaire « Uniquement cette fois » ou « Lorsque l'appli est utilisée », et non pas de manière définitive.
- **Révocation automatique en cas d'inactivité prolongée:** les applis que vous n'utilisez pas pendant un certain temps perdent automatiquement les droits d'accès aux fonctions et données sensibles, comme p. ex. à l'appareil photo ou aux contacts.

iOS (iPhone, iPad)

- **Gérer les autorisations de manière ciblée:** dans Réglages > Confidentialité et sécurité, vous pouvez sélectionner certaines catégories comme caméra, micro ou localisation et contrôler quelles applis y ont accès et éventuellement révoquer les autorisations.
- **Limitier les droits d'accès:** les accès sensibles, comme pour l'appareil photo, le micro ou la localisation peuvent être accordés de manière temporaire « Une seule fois » ou « Pendant l'utilisation de l'app », et non pas de manière définitive.
- **Consulter le rapport de confidentialité des apps:** ce rapport montre quand et comment les applis accèdent aux informations de la caméra et du micro, ainsi qu'à vos activités réseau.

