Empêcher la localisation

Tu te protèges ainsi contre l'accès à des données sensibles.

Ton téléphone portable contient de nombreux petits espions. Les trackers et les cookies dans les applications collectent en permanence des données sur toi - et les partagent avec des centaines de partenaires. Ces données peuvent également tomber dans de mauvaises mains . Une fois que les données se retrouvent sur le réseau, tu n'as plus aucun contrôle sur ce qu'il en advient.

Il existe toutefois des possibilités de se protéger et de protéger ses données contre le piratage. Quelques réglages sur le smartphone suffisent pour que la plupart des données restent entre tes mains. Les trois étapes suivantes peuvent t'aider à rester maître de ta vie privée - du débutant au professionnel.

1. Ne pas partager les données de localisation

Les données de localisation sont les données les plus précieuses que ton téléphone recueille - mais aussi les plus intimes. L'étape la plus importante est donc de ne partager tes données de localisation que lorsque c'est absolument nécessaire.

Pour ne plus partager tes données de localisation, va dans les **paramètres** et clique sur **Confidentialité et sécurité**. Clique ensuite sur **Services de localisation**. Là, tu peux désactiver les services de localisation pour toutes les applications afin de ne plus partager de données de localisation. tu peux également définir individuellement pour chaque application quand tu souhaites partager ta localisation.

Ne t’inquiète pas : les applications te solliciteront à nouveau si elles ont besoin de tes données de localisation pour une fonction spécifique, par exemple la recherche d'horaires, ou pour te trouver sur une carte. De nombreuses applications fonctionnent parfaitement sans ta localisation exacte. Tu peux lire les dernières nouvelles même si l'appli ne sait pas exactement où tu le fais.

2. Supprimer ton identifiant personnel

Tes données deviennent particulièrement intéressantes lorsqu'elles proviennent de différentes sources et qu'elles peuvent être combinées. Cela est possible grâce à un identifiant unique qui relie toutes les données que tu partages sur différentes applications. Tu peux supprimer cet identifiant. Tu rends ainsi plus difficile la combinaison de tes données.

Pour supprimer ton identifiant publicitaire (IDFA), va dans les **paramètres**, clique sur **Confidentialité et sécurité,** puis sur **Suivi**. Là, tu peux **désactiver le tracking** par les applications.

3. S'arrêter et tout refuser

Aujourd'hui, la plupart des applications et des sites web demandent s'ils peuvent collecter tes données - dans l'UE, c'est même une obligation légale. En Suisse aussi, la plupart des applis et des sites web demandent s'ils peuvent collecter tes données. Cela se fait par le biais de ce que l'on appelle des bannières de cookies, qui apparaissent lors de la première visite d'un site web - tu les connais certainement.

Les bannières de cookies sont souvent conçues de manière à ce que tu acceptes intuitivement tout et que tu envoies ainsi constamment à l'application ou au site web - et potentiellement à des centaines de fournisseurs tiers - des données dont ils n'ont en fait pas besoin. Si tu investis quelques secondes à ce moment-là, tu peux avoir un grand impact : Pour la plupart des applications et des sites web, il suffit généralement d'un clic supplémentaire sur **Préférences**, puis de cliquer sur **Refuser tout** et d'empêcher le suivi par des fournisseurs tiers.

Autres étapes

Avec les trois premières étapes, tu as déjà fait beaucoup. Une protection complète n'est pas possible. Mais il existe d'autres mesures que tu peux prendre pour protéger tes données.

- **Vérifier les autorisations :** Outre les données de localisation, tu peux également limiter l'accès des applications à d'autres données - par exemple aux données relatives à ton activité physique. Pour ce faire, clique sur **Confidentialité et sécurité dans vos paramètres.** Là, tu peux adapter les autorisations pour différentes catégories.
- **Faire le test de confidentialité de Google :** le géant de la publicité Google dispose de loin du plus grand réseau de trackers - des données d'utilisateurs de millions de sites web sont transmises à Google. Entre-temps, le groupe offre la possibilité de mieux protéger ses propres données. Avec le contrôle de confidentialité Google, tu peux vérifier rapidement et facilement quelles données te concernant sont enregistrées par le groupe et partagées avec des partenaires publicitaires - et stopper la transmission de ces données.
- **Supprimer régulièrement les cookies :** De nombreux annonceurs accèdent à tes cookies pour savoir quelles pages web tu visites et ce qui t'intéresse. Supprime donc régulièrement tes cookies via les paramètres de ton navigateur. Tu peux également configurer ton navigateur de manière à ce qu'il n'utilise qu'un minimum de cookies. Tu trouveras ici des instructions pour Chrome, Safari, Edge et Firefox.

- Installer un **bloqueur de publicité** : tu peux installer un ad-blocker dans ton navigateur, par exemple uBlock Origin. Celui-ci bloque les publicités sur la plupart des sites web et empêche les trackers de collecter tes données.
