Fiche n°11

Comment sécuriser les informations contenues dans son téléphone portable ?

Notre téléphone portable, ou smartphone, contient de plus en plus d'informations sur nous. Pourtant, contrairement à un ordinateur, nous sécurisons peu, voire pas du tout, son accès. En cas de perte ou de vol, des informations très personnelles peuvent être lues et rendues publiques. Comment faire pour protéger ses informations sur un smartphone ?

1 Noter le numéro « IMEI » du téléphone

Le code IMEI est le numéro de série unique, composé de 15 à 17 chiffres, identifiant votre téléphone. C'est en quelque sorte l'**ADN du mobile.** En cas de perte ou de vol, ce code sert à bloquer l'usage du téléphone sur tous les réseaux. Il est indiqué sur la boîte du téléphone quand on l'achète. Notez-le et gardez-le en lieu sûr (pas sur votre téléphone). Astuce : vous pouvez obtenir le code IMEI en tapant *#06# sur votre téléphone.

2 Toujours mettre en place un code « PIN »

Le code PIN (Personal Identification Number) contrôle la carte SIM (carte à puce insérée dans le téléphone) quand on allume son téléphone. Ce code **verrouille le téléphone** au bout de 3 codes erronés consécutifs. Conseil : choisissez un code compliqué. Pas votre date de naissance ni votre surnom.

3 Mettre en place un code de verrouillage du téléphone

En plus du code PIN, ce code permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps. Cela **empêche la consultation** des informations contenues dans le téléphone en cas de perte ou de vol.

4 Activer le chiffrement des sauvegardes du téléphone

Si vous pouvez faire des sauvegardes des informations contenues dans votre téléphone sur votre ordinateur, il est recommandé d'en **activer le chiffrement.** Pour cela, utilisez les réglages de la plate-forme avec laquelle vous connectez le téléphone. Cette manipulation garantira que personne ne sera en mesure d'utiliser vos données sans le mot de passe que vous avez défini. Ce chiffrement empêche un accès malveillant aux données stockées sur l'ordinateur. Il permet également d'**effacer à distance toutes les données** contenues dans un téléphone, ce qui assure une sécurité supplémentaire en cas de vol ou de perte du matériel.

5 Ne pas accepter systématiquement la géolocalisation

Il est possible de **contrôler quand et par qui on peut être géolocalisé.** Il suffit pour cela de régler les paramètres de géolocalisation du téléphone ou des applications de géolocalisation (Twitter, Facebook Lieux, Foursquare, Plyce...). Il est également possible de désactiver ou de suspendre le service de géolocalisation à tout moment, et de sélectionner les contacts qui sont autorisés à accéder aux données de localisation.
De manière générale, il est recommandé de **bien lire les conditions d'utilisation** lors de l'installation d'une application de géolocalisation. Il faut également faire attention aux messages demandant l'autorisation d'accéder à certaines informations qui apparaissent quand on lance une application.

Ne pas oublier !

L'utilisation de services de géolocalisation peut porter atteinte à la vie privée, et en particulier à la liberté d'aller et venir anonymement.

En lien

- **La fiche 4 :** Surfer en toute sécurité.
- **Les fiches « pédagogiques » :** Téléphone mobile, géolocalisation et publicité ciblée ; La géolocalisation ou le suivi des individus.

Création : Play Bac Editions Spéciales