Do not Track

Saison 1 Episode 4

Comment protéger votre smartphone
On ne va pas se mentir, protéger son smartphone, c'est quasiment mission impossible. Mais après quelques semaines à pister les trackers, voici quelques trucs que j'ai appris.

Contrôler votre smartphone

1 – Certaines de vos applications ont besoin de vos données personnelles pour fonctionner. D'autres pas. Pour faire le tri, j'ai installé Clueful de Bitdefender. C'est une appli qui vous indique quelles données sont exploitées par chacune de vos applications. Elle vous prévient si certaines le font à votre insu. Vous êtes traqués mais vous l'êtes en connaissance de cause.

2 – Avant de télécharger n'importe quoi, assurez-vous de l'utilité que vous en avez. Pensez à supprimer les applications qui ne vous sont plus utiles. Pensez à fermer celles en tâche de fond. Sur IOS, il suffit d'appuyer deux fois sur le bouton en bas de l'écran. Sur Android, vous pouvez le faire en ouvrant le menu "Applications" dans les "Paramètres".

3 – Si vous le souhaitez, vous pouvez désactiver la géolocalisation. Sur Android, il suffit d'aller dans le menu "Localisation" dans "Paramètres" et de la désactiver. En bas de la même page, vous pouvez cliquer sur "Historique des positions Google" pour désactiver cette fonction. Sur Iphone, il faut se rendre sur "Réglages" puis "Confidentialité" puis "Localisation".

4 – Le suivi publicitaire peut-être limité. Si vous avez un Android, vous trouverez un menu "Annonces" dans les "Paramètres Google". Vous pouvez désactiver "les annonces par centres d'intérêt" et réinitialiser "l'identifiant publicitaire", l'équivalent d'un cookie sur ordinateur. La méthode n'est pas infaillible puisqu'une application qui a eu accès à votre UDID reconnaîtra votre téléphone mais toutes les applis ne le font pas. Sur iPhone, le procédé est le même. Vous retrouverez les "Annonces" dans "Réglages", puis "Publicité".

Être anonyme

5 – Pour naviguer de façon tout à fait anonyme, vous pouvez télécharger Tor ou Orweb, développé par le Guardian Project. Ces services sont efficaces mais il faut être patient, le

chargement des pages est lent. Le moteur de recherche Duckduckgo.com promet de “ne pas vous espionner” et ne stocke pas d’informations personnelles sur ses utilisateurs.

6 – Ne vous connectez pas en wifi gratuit. Si c’est vraiment indispensable, dispensez-vous d’accéder à vos comptes personnels (mail, banque, réseaux sociaux etc.) Sinon, installez une application VPN (Virtual Private Network) qui vous permettra de vous connecter à Internet de manière sécurisée.

7 – Si vous souhaitez aller plus loin, n’hésitez pas à vous tenir informé sur le site du Guardian Project qui a développé des outils permettant d’anonymiser les images, de chiffrer les communications etc. Un nouvel outil, Courier, permet d’accéder à un Internet non censuré. Un bouton “PANIC” permet de la désinstaller rapidement. Elle est disponible en plusieurs langues, dont l’anglais, le chinois, le tibétain, l’ukrainien et le russe.

Zineb Dryef