Un été Sud-Ouest

À chaque jour, sa série

Tout au long de l'été, « Sud Ouest » vous offre un moment de détente. LUNDI : Sagas familiales. MARDI : Maisons d'ici. MERCREDI : En dehors des foules. JEUDI : Préparez vos mouchards ! VENDREDI : Balade œnotouristique. SAMEDI : Interdit au public. Passez un bel été « Sud Ouest » !

Le smartphone, ce drôle d'ami qui raconte votre vie

Les accros au smartphone ignorent que leur objet fétiche les espionne en permanence. Les données récoltées servent la plupart du temps à alimenter la publicité ciblée

PRÉPAREZ VOS MOUCHARDS (1/6)
Comment les nouvelles technologies trahissent tous nos faits et gestes.
DEMAIN : Balade œnotouristique chez les viticulteurs de Buzet.

DOMINIQUE RICHARD
d.richard@sudouest.fr

Au début de l'année, la police scientifique se cassait encore les dents sur les portables de certains des terroristes impliqués dans les attentats de Paris. Impossible de briser les codes des logiciels de chiffrement qui interdisaient l'accès au contenu des appareils. Rares sont cependant les utilisateurs à protéger leur vie privée de la sorte. Les stars américaines dont les photos intimes stockées dans des serveurs ont été piratées par un hacker avant d'être diffusées sur la Toile ne diront pas le contraire.

Du danger du stockage en ligne

À intervalles réguliers, des failles apparaissent dans les systèmes d'exploitation pour mobiles iOS (Apple) et Android (Google), les deux géants du numérique. Mais cela n'affole pas outre mesure les foules, tant l'addiction est forte. Les 7 milliards d'abonnés qui peuplent la planète vivent avec un petit mouchard dans la poche. Un compagnon intime à qui ils confient leurs petits secrets et qui les trahit sans vergogne à longueur de journée.

En France, 70 % des utilisateurs ne verrouillent jamais leur portable, qui reste en permanence allumé. Ils pensent n'avoir qu'un banal téléphone à la main, alors qu'ils sont en possession d'un véritable ordinateur où ils stockent massivement des données personnelles. Le plus souvent des photos et des vidéos, mais aussi – et de plus en plus – des informations médicales, bancaires ou professionnelles. Sans parler des différents codes et mots de passe qu'ils ont peur d'oublier.

Beaucoup trop importants pour être archivés dans la mémoire limitée du smartphone, ces images, fichiers et mails sont récupérés par des programmes tels que Google Drive, Dropbox ou iCloud, et partent dans le nuage informatique planétaire (cloud). La sécurité de ces informations stockées dans les centres de données géants d'Amazon, Google et compagnie échappe à leurs propriétaires.

En 2011, des chercheurs avaient découvert que les iPhone envoyaient de nuit à Apple les coordonnées des points d'accès Wi-Fi détectés dans la journée. Officiellement, il ne s'agissait pour la firme à la pomme que d'enrichir sa base de données en vue d'améliorer la rapidité des connexions. L'opération s'effectuait pourtant à l'insu des utilisateurs.

Le smartphone est avant tout un espion peu sourcilleux sur le respect de la vie privée. Sur un ordinateur, les réseaux sociaux et les petits fichiers (cookies) déposés sur le disque dur de l'internaute par les serveurs des sites visités permettent de suivre les internautes. Sur un mobile, la fuite des informations s'effectue le plus souvent par l'intermédiaire de certaines applications téléchargées sur les terminaux. Plus d'un quart d'entre elles fonctionnent comme de véritables aspirateurs à données. Elles ponctionnent les informations relatives aux autres applications installées sur l'appareil, mais surtout accèdent aux données de géolocalisation, alors que celles-ci ne leur sont a priori d'aucune utilité. Les investigations menées par l'Institut national de recherche en informatique et en automatique de Grenoble mettent surtout en cause Google, dont le modèle économique repose en partie sur la captation massive des données personnelles.

> Des sociétés spécialisées dans le traçage Wi-Fi font commerce de ces données avec l'aval des opérateurs

Les smartphones sont conçus de telle façon qu'ils facilitent le piratage de nombreuses informations, allant de l'identifiant de l'appareil aux données révélant les activités de l'utilisateur. Dirigées vers des sociétés spécialisées dans la publicité en ligne, elles servent à dessiner les profils des utilisateurs, qui seront ensuite revendus.

Le Wi-Fi, qui relie les appareils par ondes radio, n'est pas non plus un parangon de confidentialité. Lorsque le Wi-Fi est activé, le smartphone détecte en permanence les réseaux situés à proximité. Il émet périodiquement des messages où apparaissent l'identifiant du mobile, les points d'accès auxquels il s'est déjà connecté, voire des noms de lieux ou des coordonnées géographiques.

Capteurs dans les toilettes

Des sociétés spécialisées dans le traçage Wi-Fi font commerce de ces données avec l'aval des opérateurs. Lorsqu'il s'agit d'évaluer des flux routiers sur les axes de communication, l'intérêt général y trouve son compte. D'autres utilisations piétinent allègrement la vie privée. Dans un pub très fréquenté de Londres, des capteurs installés jusque dans les toilettes permettaient de déterminer la fréquence, la durée de la visite mais aussi le sexe des clients. Tout cela dans la perspective d'afficher des publicités dans les rues voisines vantant les produits que les habitants du quartier étaient susceptibles d'acheter.

L'AVIS DE L'EXPERT

ÉRIC FILIOL, ex-agent de la DGSE, directeur du laboratoire de sécurité de l'Esiea (École d'ingénieurs du monde numérique) de Laval.
« Chiffrer son téléphone, c'est la première chose à faire quand on veut protéger ses données. On trouve sur Internet les tutoriels qui expliquent la marche à suivre pour les modèles de téléphone les plus récents. Mais attention à ne pas choisir un mot de passe trop simple. Ensuite, il faut désactiver la localisation, le Bluetooth et le Wi-Fi. Et ne les remettre qu'en cas de besoin. Le Wi-Fi, c'est une porte ouverte qui permet à un attaquant de collecter énormément de données. La géolocalisation permet de vous suivre à la trace. Il faut aussi désactiver la synchronisation. Certes, elle vous permet d'accéder à tous vos fichiers à partir de n'importe quel appareil. Mais vos données ne sont plus conservées uniquement dans la mémoire du smartphone. Ils sont dans le nuage, le cloud, du système d'exploitation, et vous n'en avez plus la maîtrise complète. Là aussi, on trouve sur Internet des tutoriels compréhensibles. Les applications téléchargées doivent être certifiées et figurer au minimum dans la bibliothèque de Google Play ou d'Apple Store. Beaucoup d'applications sont intrusives et captent vos données. L'une des pires étant Facebook, ce que nous y avons découvert est inquiétant pour notre vie privée. Mais a-t-on encore une vie privée quand on utilise Facebook ? »