Les téléphones ne seront jamais sécurisés mais vous pouvez toujours essayer

Author : Hélène Molinari

Date : 28 février 2017

Je suis une femme, j'utilise mon ordinateur et mon smartphone quotidiennement mais je ne maîtrise pas tous les outils qui sont à ma disposition pour sécuriser ce dernier... On ne compte pourtant plus les mises en garde contre la géolocalisation et le traçage de nos données, donc de nos vies. Si la peur d'un monde où les humains seront tous pucés est pour le moment irrationnelle, notre société a déjà largement de quoi nous observer en permanence. Il est temps de prendre les choses en main. Cette section du Guide DIY de cybersécurité féministe du collectif HACK*BLOSSOM nous aide à y voir plus clair.

#TÉLÉPHONES

Protéger votre ordinateur portable ou de bureau c'est très bien, mais qu'en est-il des menaces contre votre vie privée et votre sécurité sur votre téléphone ? Les smartphones sont des cibles particulièrement séduisantes parce qu'ils contiennent un concentré énorme d'informations personnelles. Le GPS de votre téléphone peut traquer vos trajets tout au long de la journée. La plupart des communications avec vos amis, contenant parfois des informations sensibles ou des images, sont stockées dans des messages accessibles. Vos mails, images, vidéos, fichiers et toutes sortes de données importantes sont aussi quelques fois stockées dans vos applications.

Bien que les smartphones aient de nombreux atouts, comme leurs fonctionnalités ou leur commodité, cela veut aussi dire moins de contrôle sur votre espace numérique. Vous n'avez par le choix : vous devez faire confiance à vos applications pour utiliser vos données de façon sécurisée. Vous devez faire confiance dans la capacité de votre système d'exploitation à résister au hacking. Vous devez faire confiance à votre opérateur pour ne pas interférer avec vos données ou vos appels. Vous devez espérer que personne de malveillant ne prenne le contrôle de votre téléphone. Avant de plonger plus en profondeur, il est fondamental d'insister sur le fait que la sécurité des téléphones est bien moins développée que la sécurité de base d'un ordinateur, avec souvent moins de visibilité sur la façon dont les données sont gérées et utilisées et avec beaucoup moins d'options de sécurité. **Bien qu'il y ait beaucoup d'outils pour la sécurité des téléphones, ils ne sont pas complets et ne stopperont pas la collecte de données, la localisation ou la surveillance.**

Avec autant de risques pour vos informations personnelles, comment pouvez-vous encore utiliser votre smartphone sans prendre des mesures pour vous protéger ? **Chiffrez ! Chiffrez ! Chiffrez !** Quand vous sécurisez votre environnement numérique, c'est important de reconnaître que les applications ne sont pas toujours une menace pour votre sécurité : elles peuvent aussi être un atout. Certaines des données les plus sensibles sur votre téléphone, de vos photos à vos sms ou votre navigation peuvent être sécurisées à un degré correct. Et la technique à suivre la plus évidente est la plus connue : le chiffrement !

En chiffrant votre téléphone et les données qui s'y trouvent, vous aurez une plus grande assurance au cas où quelque chose arriverait à votre téléphone (qu'il soit volé ou hacké), vous aurez toujours des protections mises en place. Nous allons vous proposer quelques recommandations sur différentes façons de chiffrer vos fichiers, sms et même vos appels.

Protégez vos données : le chiffrement sur iOS et Android

Tout comme vous chiffrez votre ordinateur pour que personne ne puisse fouiller sur votre disque dur sans mot de passe, vous pouvez chiffrer votre téléphone. C'est d'autant plus important que s'il était amené à être volé ou confisqué, vous ne voudriez définitivement pas que quelqu'un puisse avoir librement accès à vos photos, vidéos, sms et contacts. iOS et Android ont différentes façon de le faire, donc n'hésitez pas à lire celle qui vous semble la plus appropriée pour vous (notez que iOS8 active le chiffrement par défaut, mais pas les versions antérieures). Nous vous proposons des super guides qui vous expliqueront le processus bien mieux que nous :)

Le chiffrement sur iOS via les instructions de l'Electronic Frontier Foundation
Le chiffrement sur Android via le guide de Greenbot

Protégez vos sms

Les sms peuvent contenir les échanges les plus privés et personnels de vos communications. Ils sont aussi particulièrement vulnérables : votre opérateur téléphonique peut les lire lorsqu'ils sont envoyés (comme n'importe quelle agence gouvernementale qui entretient de bonnes relations avec le fournisseur). N'importe qui ayant accès à votre téléphone peut aussi les lire (avec un peu de chance vous avez chiffré votre téléphone pour l'éviter !). Heureusement pour vous, il existe de nombreuses applications qui chiffrent vos sms sur iOS et Android pour vous garantir des conversations vraiment privées.

Signal

Signal est une application gratuite et open source qui chiffre vos sms grâce aux gourous de la sécurité de l'Open Whisper Systems. Quand vous envoyez un sms à un-e ami-e qui utilise aussi Signal, le sms sera chiffré pour que vous seuls puissiez lire les sms sur vos téléphones. Ça se fait automatiquement, sans effort de votre part ! Et la seule information disponible pour ceux qui surveilleraient le réseau téléphonique est : qui a envoyé le sms, qui l'a reçu et quand il a été reçu. Ils ne peuvent pas voir le contenu.

Les sms envoyés aux amis n'utilisant pas Signal ne seront pas chiffrés, mais le fait d'avoir cette option fait de cette application l'outil parfait pour envoyer vos sms. Ce qui est particulièrement génial c'est que peu importe si vos messages étaient chiffrés pour le destinataire, ils le seront localement sur votre téléphone. Donc si quelqu'un contrôle votre téléphone, il-elle devra toujours déchiffrer l'application (et votre téléphone !) pour voir vos messages stockés (ce que la grande majorité des voleurs et hackeurs ne savent pas faire).

L'Electronic Frontier Foundation offre des guides pour l'utilisation de Signal sur iOS ou Signal sur Android.

Protégez vos appels

La mise sur écoute est quasiment une tradition américaine. Si vous vous retrouvez dans des situations où vous ne vous sentez pas à l'aise ou en sécurité à l'idée que votre appel soit surveillé, vous devriez envisager d'utiliser une application dont la spécialité est de chiffrer vos appels. La plupart le fait en envoyant votre conversation sur une connexion de données plutôt que par le réseau téléphonique, permettant donc de chiffrer les 1 et les 0 avant d'arriver à votre destinataire.

Applications de chiffrement d'appels

Nous vous recommandons d'utiliser **Signal**, qui est disponible sur iOS et Android. Les deux sont gratuits, open source et développés par la fantastique équipe de l'Open Whisper Systems.

Notez bien que les appels chiffrés ne fonctionnent que si la personne que vous appelez utilise aussi ces applications. Soyez aussi conscient-e que le son est un peu plus mauvais quand les appels sont chiffrés.

L'Electronic Frontier Foundation propose des guides d'utilisation de Signal pour iOS et pour Android.

Protégez votre navigation sur smartphone

Vous avez de la chance ! Vous avez à disposition de nombreuses options faciles et efficaces pour sécuriser votre navigation sur téléphone. Jetez un œil à la section navigation sur téléphone et téléchargez Firefox Focus pour iOS ou Firefox pour Android.

Dans une section précédente du guide (#ANONYMAT), nous avons évoqué la sécurisation de votre navigation avec un VPN. Heureusement, vous pouvez aussi utiliser un VPN sur votre téléphone ! Si vous avez déjà un fournisseur, c'est relativement facile de l'installer sur votre téléphone. Suivez les instructions d'Apple pour iOS ou allez voir OpenVPN (le client VPN que nous vous recommandons pour Android).

Suivez les instructions d'Apple pour configurer votre VPN sur iOS

Installez OpenVPN pour activer le VPN sur Android

Quelques réflexions sur la sécurité des téléphones

Vous avez minutieusement vérifier toutes vos applications. Vous chiffrez votre téléphone, vos sms et même certains de vos appels. Votre téléphone est une forteresse ! Vraiment ?

La chose la plus fondamentale à retenir est qu'aucun téléphone n'est sécurisé à 100%. Si vous vous retrouvez un jour dans une situation où vous devez absolument vous protéger, comme par exemple vous rendre à un événement avec une forte présence policière ou éviter un prédateur ou un agresseur, envisagez de laisser votre téléphone à la maison jusqu'à être en sécurité. Éteindre votre téléphone pendant un moment, et ensuite le rallumer, déclenche en fait des programmes de surveillance gouvernementaux, donc n'essayez pas de le faire si vous allez à une manifestation ou autre. Envisagez plutôt d'acheter un téléphone prépayé si vous en avez les moyens. Ces approches ne sont pas toujours possibles ; ce guide ne peut pas vous dire ce qui vous convient. Mais c'est à vous de gérer votre espace numérique : peu importe l'action que vous déciderez de prendre, ce sera la bonne.

#INTRODUCTION

#ANONYMAT

#HACKING

#DATA

#SOCIAL

#CHEAT SHEET