Je sécurise mon téléphone

Je me protège des dispositifs de surveillance

Des conseils pour se protéger, repérer et supprimer des logiciels de surveillance de son téléphone

Retour

Points de vigilance

Les logiciels de surveillance permettent de surveiller à distance les activités, les communications et les déplacements d'une personne sans son accord/sans qu'elle ne s'en rende compte. Ces logiciels peuvent donner accès à différentes fonctionnalités : appels, messages, photos, vidéos, localisation, utilisation des applications, etc.

Ces moyens de surveillance peuvent être de plusieurs types :

1) Les logiciels espions installés sur le téléphone de la victime, difficilement détectables. Ils sont illégaux mais peuvent être achetés en ligne. Cependant, pour les installer l'agresseur a besoin d'avoir un accès physique au téléphone.

Conseils

Je me protège des dispositifs de surveillance :

Il faut rendre complexe l'accès à son téléphone et renforcer ses mots de passe :

Changez le *code PIN* de la *carte SIM*, si vous pensez que quelqu'un peut le connaitre (ici sur Apple et ici sur Android).

Utilisez un code de déverrouillage du téléphone afin que votre téléphone se verrouille après une certaine période d'inactivité (ici sur Apple et ici sur Android). Paramétrez votre téléphone de façon à ce que ce verrouillage automatique s'effectue après une période d'inactivité courte, idéalement 30 secondes ou 1 minute (ici sur Apple et ici sur Android). Si possible, utilisez les empreintes digitales pour déverrouiller votre smartphone.

Renforcez le mot de passe de votre *Cloud* en suivant ces 5 conseils simples.

Pour réduire la diffusion d'informations à partir de votre téléphone, désactivez l'accès de vos applications à votre géolocalisation et activez-la seulement quand vous en avez besoin (ici sur Apple et ici sur Android). De même, utilisez le *mode avion* ou désactivez le *Wi-Fi*, les données mobiles, le *Bluetooth* et le *GPS* lorsque vous ne les utilisez pas (sur Apple/sur Android).

Bon à savoir : Si vous utilisez un iPhone avec iOS14, vous pouvez plus facilement voir si certains services sont actifs sans votre autorisation (services de géolocalisation, autorisation d'accès à la caméra…) : lire l'article ici. Si vous utilisez un Android, Android version 11 permet également de paramétrer de nombreux éléments pour la vie privée et la sécurité : lire l'article ici.

Parmi les dispositifs de surveillance, il existe aussi des **balises/traceurs GPS** et qui peuvent être utilisés par l'agresseur pour géolocaliser la victime à son insu et qui sont reliées au téléphone de l'agresseur : retrouvez ici plus d'informations.

Je repère si un logiciel espion est installé sur mon téléphone :

Si votre partenaire (ou ex) violent est au courant de choses que vous ne lui avez jamais dites, il se peut qu'il ait eu accès à des informations sur votre smartphone, votre ordinateur ou vos comptes internet ou réseaux sociaux.

Redoublez de vigilance si votre téléphone vous a été offert par votre partenaire. Réfléchissez également si votre partenaire a pu avoir en main votre smartphone et le manipuler pendant quelques minutes (temps durant lequel un logiciel espion aurait été physiquement installé sur votre appareil).

Même si un logiciel espion est par principe caché, **soyez à l'affût de tout**

JE PROTÈGE
MA VIE PRIVÉE
EN LIGNE

téléphone. Le logiciel espion n'apparaît pas explicitement dans la liste des applications : il se dissimule en prenant le nom et le logo d'autres applications : Calculatrice, Horloge, convertisseur de devise, ou des applications système (mise à jour du téléphone, gestionnaire de la batterie) par exemple, *System Service* ou *Update Service*. Une vraie application système ne peut pas être désinstallée. Si vous ne reconnaissez pas une application, cela peut être le signe d'un logiciel espion.

Vérifiez si un **magasin d'applications alternatif est installé sur votre téléphone** (Cydia, Sileo, ou Zebra pour Apple et F-Droid pour Android), ce qui montre qu'il a été *débridé* (ou jailbreaké).

Installez un antivirus sur votre téléphone Android *(il n'est pas possible d'installer un antivirus sur iPhone)*, et lancez le scan de l'appareil. En effet, la plupart des logiciels de protection incluent la détection de logiciels espions (ex : Malwarebytes, Avast Mobile Security, Zone Alarm...).

⚠ **Attention : si une personne a en effet installé un logiciel espion sur votre téléphone**, ou si elle a accès à votre téléphone d'une autre manière, **elle pourra être informée de l'installation d'un anti-virus**. Si vous craignez des représailles, **nous vous conseillons d'être accompagnée** par une structure spécialisée. Si vous vivez des (cyber)violences commises par votre partenaire ou ex, vous trouverez plus d'informations ici.

Je supprime un logiciel espion de mon téléphone :

Gardez à l'esprit que lorsque vous supprimez un logiciel de surveillance, la personne qui vous surveille peut en être informée. Si vous craignez des représailles, évitez de le supprimer pour le moment et adressez-vous à une structure qui vous aidera à élaborer une stratégie de sécurité.

Vous pouvez déconnecter vos comptes Cloud et **remettre le téléphone aux paramètres d'usine.** Cela supprimera toutes les données et applications du téléphone.

⚠ Que vous désinstalliez le logiciel espion ou restauriez votre téléphone aux paramètres d'usine, il est important de **sauvegarder au préalable** vos contacts et informations personnelles ainsi que des éléments qui peuvent être utilisés comme preuves. Pour sauvegarder des photos, faites une sauvegarde manuelle en branchant votre téléphone à votre ordinateur. Sur Android, vous pouvez sauvegarder vos contacts directement sur votre carte SIM.

⚠ **Attention : s'il n'y a pas de logiciel espion, il peut tout de même y avoir d'autres formes de surveillance :** si la personne a un accès physique au smartphone, si elle a accès au compte Cloud via le mot de passe : voir "comment protéger votre cloud", ou en faisant un usage détourné d'applications préinstallées (Google Maps, Localiser mon téléphone, etc.).

⚠ **Au-delà des logiciels espions, d'autres logiciels malveillants (chevaux de Troie, virus...) peuvent vous être envoyés pour nuire à vos appareils ou obtenir des informations personnelles.**

Ne cliquez pas sur des liens inconnus qui peuvent vous être envoyés.

Repérez les tentatives de piratage par email

JE PROTÈGE
MA VIE PRIVÉE
EN LIGNE