Cyber protection, comment faire ? (doc à compléter 09/09/2019)

Protection

 Enlever la géolocalisation des appareils numériques (tablette, smartphone, ipod,…). Ne l'utiliser que lorsque c'est nécessaire (le temps de l 'utilisation du GPS par exemple), **sur les appareils de l'adulte et ceux des enfants** (pour info, sans internet, il est moins facile d'être localisé, donc si possible : se déconnecter).

Vérifier les paramètres de sécurité de tous les comptes accessibles à distance (confidentialité, géolocalisation, autorisation des applications…).

- Mettre à jour tous **les mots de passe** (dont ceux des adresses mails de secours), les questions de **confidentialité** et les adresse de sauvegarde des comptes informatiques (dont les mails), téléphoniques (portable, box à re-paramétrer) et bancaires mais aussi CAF, pôle emploi, impôts, cpam, réseaux sociaux de l'adulte et des enfants.
- Vérifier l'identité et les accès au compte du fournisseur téléphone et internet. La personne doit s'assurer d'être le propriétaire de la ligne, elle doit avoir ses propres identifiants et mot de passe, sur un compte **individuel**.
- En cas de doute sur la présence d'un logiciel ou application espion (l'appareil est susceptible d'avoir été manipulé par le conjoint, le conjoint a des habiletés particulières en informatique, numérique, appareil qui semble anormalement lent…) sauvegarder les fichiers personnels importants (photos, vidéos, documents) et réinitialiser l'appareil sur les paramètres d'usine. Attention cette manipulation **efface toutes les données personnelles installées après l'achat et toutes les mises à jour effectuées depuis**.

  Un antivirus à jour, sur l'ordinateur et/ou le téléphone, peut repèrer les logiciels espions.
- Idéalement, ne télécharger que des applications des systèmes IOS ou Android (en fonction du téléphone), pas d'autres applications téléchargeables sur internet car peu sûres.
- Cacher la web cam lorsqu'elle n'est pas en cours d'utilisation.
- Fermer les fenêtres actives et se déconnecter de ses comptes lorsque d'autres personnes peuvent utiliser le matériel.
- Possibilité de dénoncer certains comportements d'une personne à la « Police des Réseaux » (aller dans « mentions légales » tout en bas de la page informatique généralement), qui peut retirer la personne du réseau.

Preuves

- Faire des captures d'écran.
- Installer un logiciel de sauvegarde des sms, comme SMS back up (https://www.commentcamarche.net/faq/38937-sauvegarder-les-sms-sous-android).
  Attention cette procédure ne fonctionne que pour les smartphones !
- Certaines émoticônes d'apparence banale sont en fait des allusions sexuelles qui peuvent être prises en compte dans les cas de harcèlement sexuel lorsqu'elles sont répétées (https://www.20minutes.fr/arts-stars/culture/2319231-20180810-aubergine-peche-taco-comment-parler-sexe-emojis) (A vérifier : la retranscription de ces émoticônes lorsque les sms sont basculés vers la messagerie mail. Si cela pose un problème, il faudra alors penser à faire des captures d'écran pour ses sms particuliers)
- Créer dans sa messagerie (**après avoir vérifié la sécurisation de l'accès**) un dossier de sauvegarde des éléments d'identité (copie des pièces d'identité, cpam, mutuelle, permis…) et des documents importants (impôts, santé, certificats médicaux, scan des dépôts de plainte, main courante, jugement, audience jaf, …)
- Parfois, des mouchards peuvent être installés sur les véhicules, par exemple. Cela peut expliquer la géolocalisation.

Je sécurise mon téléphone

Je me protège des logiciels de surveillance

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

Points de vigilance

Les logiciels de surveillance permettent de surveiller à distance les activités, les communications et les déplacements d'une personne : 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. Les logiciels les plus utilisés sont Hoverwatch, mSpy, Snoopza, FoneMonitor et Spyzie. Ils sont illégaux mais peuvent être achetés en ligne. Cependant, pour les installer l'agresseur a besoin d'avoir un accès physique au téléphone.

2. Les applications de surveillance légales, comme celles de surveillance parentale, peuvent être détournées. Il est facile de les repérer sur son téléphone.

3. Il est possible d'accéder aux informations personnelles via le compte Cloud (contacts, communications, photos, etc) de quelqu'un-e, à condition d'en connaître le mot de passe.

4. Plusieurs applications préinstallées sur les téléphones (Google Maps, Google Drive, ou les applications pour retrouver son appareil en cas de perte/vol comme l'application "Localiser mon téléphone") peuvent être activées à distance et transmettre des données sur les déplacements. Il faut cependant qu'une personne malveillante ait eu accès à votre téléphone pour les configurer.

Conseils

Pour se protéger de ces logiciels 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 (sur Apple/sur Android)
- Utilisez un code d'accès afin que votre téléphone se verrouille après une certaine période d'inactivité (sur Apple/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 (sur Apple/sur Android).
- 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 (sur Apple/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).
- Il est possible de se rendre dans des magasins agréés pour vérifier la présence d'un logiciel espion sur son téléphone (démarche payante).

Pour repérer si un logiciel espion est installé sur son téléphone :

- Même si un logiciel espion est par principe caché et n'est pas visible dans la liste d'applications de votre portable, soyez à l'affût de tout fonctionnement suspect qui pourrait indiquer la présence d'un logiciel espion (par exemple, si votre téléphone chauffe, s'il est plus lent que d'habitude, si sa batterie tient beaucoup moins bien et/ou si votre mémoire est saturée).
- Un autre indice est qu'un store alternatif est installé sur votre téléphone (Cydia pour Apple et F-Droid pour Android), ce qui montre qu'il a été débridé.
- La plupart des logiciels de protection incluent la détection de logiciels espions (ex : Avast Mobile Security, ZoneAlarm…)

Pour supprimer un logiciel espion de son téléphone :

- Vous pouvez déconnecter vos comptes Cloud et remettre le téléphone aux paramètres d'usine (sur Apple/sur Android). Cela supprimera toutes les données et applications du téléphone et annulera le débridage.
- En cas de doute supplémentaire, il peut être prudent de vous adresser à un-e professionnel-le du numérique ou changer de téléphone, si cela vous est possible.
- Dans les deux cas, il est important de sauvegarder au préalable vos contacts et informations personnelles ainsi que des éléments qui peuvent être utilisés comme preuves dans une éventuelle procédure judiciaire.
- 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. Pour cela, essayez de trouver un téléphone sécurisé : téléphone public, d'un-e ami-e de confiance…

Au-delà des logiciels espions, des virus et d'autres logiciels malveillants 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.
- Soyez vigilante quand vous utilisez les Wi-Fi publics.