PROTOCOLE DE SÉCURITÉ NUMÉRIQUE

un guide de sécurité de base
pour toutes et tous

internationalistcommune.com

Protocole de sécurité numérique

un guide de sécurité de base pour toutes et tous

internationalistcommune.com

Protocole d'information sur la sécurité numérique

Nous utilisons tous les jours nos téléphones, tablettes ou smartphones, ainsi que nos ordinateurs et nos appareils photo. Par conséquent, notre sécurité lorsque nous les utilisons est un sujet très important auquel nous devons nous confronter. En particulier pour les personnes qui s'organisent et luttent contre le système capitaliste, la sécurité et l'autodéfense sont des sujets essentiels qui devraient également être pris en considération au niveau numérique. Avec l'utilisation quotidienne de ces appareils, nous pouvons devenir vulnérables face à l'État ou à quiconque voudrait nous nuire. Lorsque nous recevons un appel, lorsque nous utilisons l'internet, lorsque nous envoyons des messages, nous laissons des traces numériques que l'ennemi peut ensuite utiliser contre nous. **Ce protocole a pour but de présenter les principales menaces et de proposer des solutions avec des ressources pour s'adapter et se protéger de manière efficace.**

La sécurité numérique pour quoi faire ?

En matière de sécurité numérique, il est important de se poser quelques questions afin de comprendre pourquoi certaines mesures doivent être prises pour notre protection et quel est leur impact. Nous pouvons ainsi éviter de devenir paranoïaques ou de devenir une cible facile pour l'ennemi. Les questions suivantes sont donc importantes pour nous.

Pourquoi est-il important de veiller à notre sécurité ?

Se protéger soi-même, protéger ses appareils, son téléphone et ses ordinateurs, c'est aussi protéger ses camarades, son collectif ou son organisation. La cybersécurité n'est pas une question individuelle et nous sommes responsables non seulement de notre sécurité, mais aussi de celle de nos camarades.

Quelles sont les informations que je veux protéger ?

Mon identité, mes recherches sur Internet, mon activité sur les réseaux sociaux, en général ma localisation ou ma présence dans un certain lieu, mes communications, les canaux d'information, les publications sur Internet...

De qui je veux me protéger, de quels ennemis ?

Des inconnus, des services de renseignement des Etats, d'autres Etats, des banquiers, des hackers, des services de police judiciaire, des voleurs, de conjoint violent, de mon opérateur de téléphonie mobile ou de mon fournisseur d'accès à internet, etc...

Quels types d'attaques ?

Lorsque l'ennemi a un accès direct après avoir saisi mon téléphone par perquisition, lorsque l'ennemi me cherche sur Internet, lorsqu'un ennemi tente de pirater mon ordinateur, lorsque mon ennemi demande des informations à mon opérateur téléphonique ...

Nous voulons mieux comprendre tout cela. Commençons donc par les traces utilisables que nous laissons sur nos appareils (téléphone/ordinateur) et nous pourrons ensuite les examiner lors de nos connexions à l'internet. C'est pourquoi nous verrons comment nous laissons des traces sur les ordinateurs et quels sont les systèmes d'exploitation (logiciels qui gèrent le matériel et les applications d'un ordinateur) existants et en quoi ils diffèrent les uns des autres en termes de sécurité et d'utilisation. Nous ferons de même pour les téléphones et nous verrons pourquoi et comment utiliser les VPN (Virtual Private Network). Nous comprendrons quels sont les types d'attaques de l'ennemi et comment nous pouvons nous en protéger. Cela signifie que nous vous présenterons également des méthodes d'utilisation sécurisée et de bonnes pratiques pour les appareils avec lesquels nous travaillons quotidiennement.

Ordinateurs

Sur les ordinateurs, nous laissons des traces exploitables lorsque:

- Nous stockons des fichiers (vidéos/photos/sons/documents...) sur un disque dur (interne ou externe), sur des clés USB et sur des cartes SD.

- Nous nous connectons à Internet pour aller sur des sites web, utiliser des applications connectées (messagerie, emails, applications de jeux et de médias numériques comme Instagram etc.), télécharger des fichiers (photo/vidéo/son/document, etc.).

Systèmes d'exploitation

Le système d'exploitation joue un rôle très important dans l'ordinateur. Il est chargé de faire fonctionner ensemble toutes les parties de l'ordinateur telles que la mémoire, le processeur et le stockage. C'est également le système d'exploitation qui traduit le langage de l'ordinateur en un langage que nous pouvons comprendre. Un ordinateur sans système d'exploitation est inutile. Les logiciels peuvent être considérés comme des facilitateurs permettant d'effectuer une tâche sur l'ordinateur. Par exemple, si vous avez besoin d'envoyer un message, vous pouvez installer une application qui envoie des messages. Le logiciel est cette application. Le terme logiciel est utilisé pour le différencier du matériel, c'est-à-dire des composants physiques d'un système informatique. Il existe différents systèmes d'exploitation, qui n'offrent pas tous les mêmes possibilités. Certains de ces systèmes d'exploitation sont des systèmes d'exploitation à source ouverte. Cela signifie qu'il s'agit d'un système d'exploitation ou d'un logiciel développé en collaboration et que tout le monde peut l'utiliser, le modifier et le distribuer.

- Windows:

Il s'agit d'un système d'exploitation développé par la société Microsoft qui collabore avec les services de l'État dans le monde entier. Il peut être utile pour utiliser des logiciels privés de création de contenu (comme Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.) Mais il est impossible de savoir comment les données informatiques sont traitées par l'entreprise. Elle ne fournit pas ses algorithmes, ses sources et ne permet pas de sécuriser le disque dur, il est très facile de casser le mot de passe et de s'introduire dans vos données. En tant qu'entreprise capitaliste, elle peut vendre les informations de ses utilisateurs à des Etats (comme la Turquie) en échange de l'accessibilité de ses services dans les pays collaborateurs.

- macOS:

Il s'agit d'un système d'exploitation développé par la société Apple Inc. Tout comme Windows, il est impossible de savoir comment les données de votre ordinateur sont traitées par l'entreprise. Mais il est aussi utile pour utiliser des logiciels de création de contenu privés (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.). Il ne fournit pas ses algorithmes (ses sources) et ne permet pas de sécuriser le disque dur. Il est difficile de casser le mot de passe et de s'introduire dans vos données. Apple affirme ne pas vendre de données personnelles à des tiers. En tant que forces anticapitalistes, nous devons prendre des précautions et ne pas croire ces entreprises.

- Linux:

Il s'agit d'un système d'exploitation à source ouverte qui comporte plusieurs suites disponibles (par exemple Debian, Ubuntu, etc.). Il a été développé par Linus Torvalds et est basé sur les systèmes d'exploitation Unix.

Il n'est pas compatible avec l'utilisation de logiciels de création de contenu privés (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro ...). Il existe toutes sortes d'applications open source qui peuvent être utilisées pour la création de contenu privé comme alternative et tout autre travail comme la communication etc. de manière sécurisée et privée disponible pour ce système d'exploitation. Tous les algorithmes (leurs sources) sont accessibles en ligne et régulièrement vérifiés par des personnes du monde entier. Il est possible de crypter en toute sécurité le disque dur et tout autre système de stockage. Avec une bonne phrase de passe, il est (très) difficile de casser une longue phrase de passe. Cela signifie qu'il est très coûteux en temps et en énergie, et donc en argent, pour un ennemi qui veut s'emparer de vos données. En outre, de nombreuses applications utiles pour le nettoyage des données et la navigation (détaillées plus loin) sont préinstallées. C'est le plus efficace des systèmes pour éviter les logiciels malveillants et les virus. Pour ces raisons, il est recommandé de l'utiliser à la place de Windows/MacOS. Ici vous pouvez en savoir plus.

https://ubuntu.com/download/desktop
https://www.linux.org/pages/download/

- TAILS (The Amnesic Incognito Live System):

Il s'agit d'un système d'exploitation qui a été développé pour garantir un niveau élevé de sécurité et d'anonymat lors de la navigation sur l'internet et de l'archivage. Il s'agit d'un système vivant. Cela signifie que vous pouvez l'installer sur une clé USB ou une carte SD et l'utiliser sur tous les ordinateurs (mais pas sur tous les Macbooks), sans utiliser le système informatique d'origine (Windows/Linux...). Vous ne laissez donc aucune trace, sauf si vous le souhaitez. Sa fonction amnésique (il perd toute mémoire) permet de ne rien garder sur l'ordinateur. Il se connecte à l'internet par le biais du navigateur Tor. Il est recommandé par la plupart des Lanceur.euses d'alerte (personne révélant des informations sur l'activité d'une organisation) et a été financé par le projet Tor (https://www.torproject.org/). Basé sur une structure Linux, avec une bonne phrase de passe, il est (très) difficile de casser le mot de passe.

Voici sa documentation et le tutoriel pour son installation: https://tails.net/

Téléphones

Sur un téléphone/tablette, nous laissons des traces exploitables lorsque:

- nous communiquons par SMS/appel (via un opérateur téléphonique)
- Nous prenons des photos/vidéos/sons
- Nous utilisons des applications de localisation
- Nous stockons des fichiers (vidéos/photos/documents) sur le téléphone ou la mini carte SD
- On se connecte à l'internet pour aller sur des sites web, utiliser des applications connectées (messagerie, emails, etc.), télécharger des fichiers (photo/vidéo/son/document...)

Il existe différents systèmes d'exploitation pour téléphones, qui ne permettent pas tous les mêmes possibilités:

- iOS:

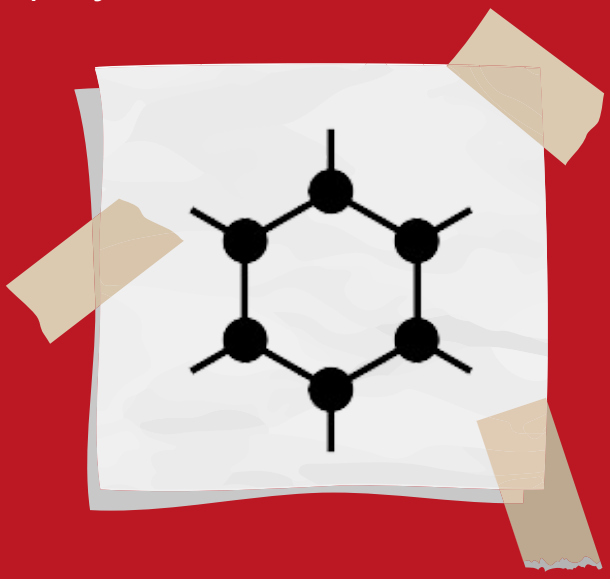
C'est un système d'exploitation mobile pour iPhone développé par Apple Inc. Il est impossible de savoir comment les données téléphoniques sont traitées par l'entreprise.

- Android:

C'est un système d'exploitation mobile utilisé sur la plupart des téléphones (Samsung, Huawei, Redmi, etc.). Il n'offre pas une bonne sécurité contre le piratage. Il est impossible de savoir comment les données du téléphone sont traitées.

- GrapheneOS:

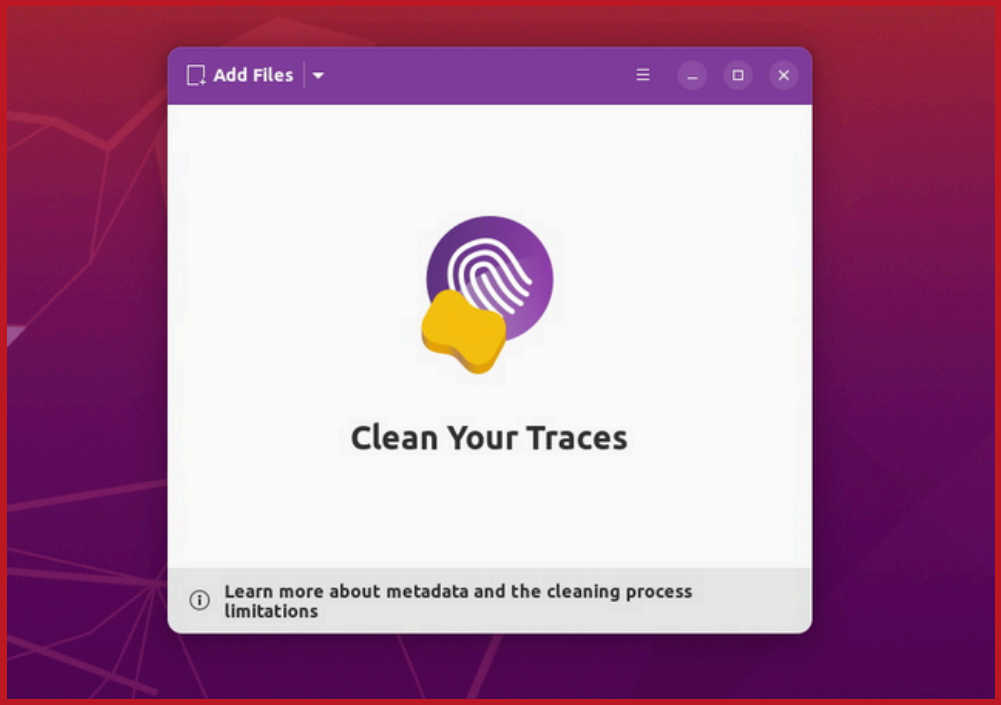
C'est un système d'exploitation mobile open source qui ne prend en charge que les téléphones Google Pixel. Il est recommandé d'utiliser les nouvelles séries Pixel (6, 6a, 6pro, 7, 7a ...).
Ce système d'exploitation remplace le système d'exploitation d'origine. Il permet d'éviter la surveillance de Google et de chiffrer le contenu de son téléphone grâce à un système développé par des camarades. Il est compatible avec la plupart des applications Android et propose également des alternatives open source. Il a été développé en tant que projet alternatif à but non lucratif. Grâce à la protection de la vie privée et à la sécurité qu'il offre, il rend l'exploitation des sources de vulnérabilité les plus courantes beaucoup plus difficile. Il améliore la sécurité du système d'exploitation et des applications qui tournent dessus.



GrapheneOS ajoute divers paramètres pour des fonctions telles que l'autorisation du réseau, l'autorisation des capteurs (microphone, appareil photo, etc.), des restrictions lorsque l'appareil est verrouillé (broches USB-C/pogo, appareil photo, paramètres des tuiles rapides, etc.) ainsi que des fonctions de confidentialité et de sécurité plus complexes destinées à l'utilisateur. Il est recommandé d'installer GrapheneOS pour une utilisation sécurisée des téléphones.

À Propos du Stockage

Chaque fichier (vidéo, photo, pdf, etc.) contient des métadonnées qui sont des informations sur sa date de création, sa modification, sa taille, l'appareil photo, le format, l'application utilisée pour le créer et le modifier. La géolocalisation est également une métadonnée. Il s'agit du processus de détermination de l'emplacement physique d'un appareil à l'aide de technologies telles que le GPS, le Wi-Fi ou les réseaux cellulaires. Elle fournit des informations sur l'emplacement d'un appareil, souvent exprimées sous forme de coordonnées ou d'adresse physique. Il est recommandé de vérifier votre appareil afin de rendre difficile l'accès à son contenu. Il existe un risque constant de diffusion des métadonnées des fichiers par courriel/SMS/réseaux sociaux. Il est souhaitable de les supprimer, surtout en cas de publication sur l'internet ou de partage (par message ou courriel). Il existe pour cela l'application Metadata Cleaner sur Tails/Debian/Linux ou, sur téléphone, l'application Image Pipe.



1. Comment éviter la diffusion d'informations sur l'internet?

Lorsque l'on utilise l'internet, de nombreuses informations circulent et sont conservées pendant plusieurs années. Celles-ci varient selon le site web que l'on visite, le téléphone que l'on utilise, le réseau Wi-Fi, le partage de la connexion internet, etc. Il existe des solutions pour réduire l'espionnage et l'identification lors de la navigation sur internet.

VPN

Le rôle du VPN (Virtual Private Network) est de dissimuler l'emplacement de votre connexion et de garantir une meilleure protection de vos informations. Le VPN établit une connexion sécurisée et fiable au-dessus d'un réseau non sécurisé, protégeant ainsi votre activité en ligne, votre localisation et votre identité.

Comment cela fonctionne-t-il?
Lorsque vous vous connectez à l'internet, chaque connexion a une adresse qui lui est attribuée. Par exemple, si vous êtes connecté à l'internet chez vous, cette connexion a une adresse, un code, et toute personne qui se connecte sera identifiée comme étant présente à cette adresse. Cette adresse est appelée adresse IP. C'est là le danger, si l'ennemi sait quel est votre appareil et s'il vous espionne, votre localisation réelle sera facilement identifiée, lorsque vous vous connectez à un réseau sans utiliser de VPN, exposant votre localisation et le fait qu'il s'agit d'un lieu de camarades.

La fonction du VPN est de changer cette adresse et de cacher les informations envoyées, ce qui rend le travail de l'ennemi pratiquement impossible. Le VPN place vos informations dans une boîte protégée par une clé. Si l'ennemi tente d'intercepter vos informations par le biais de l'espionnage numérique, il ne pourra pas ouvrir cette boîte.

Certains fournisseurs de VPN ne sont pas payants et sont totalement anonymes, comme RiseUp VPN, qui peut être installé sur n'importe quel appareil. Le VPN RiseUp n'est pas compatible avec les appareils Apple iOS. Le VPN Proton mail fonctionne également sans payer sur iOS mais nécessite une connexion mail sur certains appareils. D'autres fournisseurs qui sont sécurisés, comme Mullvad, PIA etc, sont payants mais sont également bons et sécurisés.

When you use a VPN

Tor Browser

Le navigateur TOR est la meilleure solution pour effectuer des recherches, regarder des vidéos ou publier sur Internet de manière simple et sécurisée. Il n'y a pas d'historique de navigation pas d'enregistrement de mot de passe et il permet de cacher à l'opérateur Internet et aux sites visités, l'identité de l'utilisateur. Il utilise plusieurs points de relais qui permettent d'anonymiser nos connexions et notre travail.

Il est disponible sur tous les téléphones et ordinateurs:
https://www.torproject.org/

2. Ce dont il faut se protéger?

Il est difficile de vérifier si un composant d'un téléphone a été physiquement modifié et/ou corrompu par des ennemis. Nous avons autour de nous des milliers d'appareils électroniques tels que des téléphones, des ordinateurs, etc. Qui plus est, la plupart de nos communications passent par ces mêmes appareils. Plus encore, la plupart de nos communications passent par ces mêmes appareils. Il est donc d'autant plus nécessaire de les utiliser de manière sûre et consciente pour se défendre contre les menaces en ligne. Les menaces en ligne sont un ensemble de pratiques et de techniques visant à envahir les appareils, à espionner, à collecter et à modifier des données. Pour contrer ces menaces, la sécurité numérique est constituée de techniques et de pratiques qui rendent l'utilisation de la technologie plus sûre.

Types d'Attaques

Logiciels malveillants - Malware

Les logiciels malveillants sont des logiciels conçus pour nuire à un ordinateur. Les logiciels malveillants peuvent voler des informations sensibles sur votre ordinateur, ralentir progressivement votre ordinateur ou même envoyer de faux courriels à partir de votre compte de messagerie à votre insu.

Voici quelques types de logiciels malveillants dont vous avez peut-être entendu parler:

- **Virus :** Un programme informatique nuisible qui peut se copier lui-même et infecter un ordinateur.

- Ver : Programme informatique malveillant qui envoie des copies de lui-même à d'autres ordinateurs via un réseau.

- Spyware (logiciel espion) : Logiciel malveillant qui recueille des informations sur les personnes à leur insu.

- Adware (logiciel publicitaire) : Logiciel qui joue, affiche ou télécharge automatiquement des publicités sur un ordinateur.

- Cheval de Troie : Programme destructeur qui prétend être une application utile, mais qui nuit à votre ordinateur ou vole vos informations après son installation.

Comment les logiciels malveillants se propagent-ils:

- Téléchargement de programmes sur l'internet qui contiennent secrètement des logiciels malveillants
- Visite d'un site web infecté par des logiciels malveillants
- Cliquer sur un faux message d'erreur ou une fenêtre contextuelle qui lance le téléchargement d'un logiciel malveillant.
- Ouverture d'une pièce jointe à un courrier électronique contenant des logiciels malveillants
- par le biais de clés USB et de disques durs

Les logiciels malveillants peuvent se propager de nombreuses manières différentes, mais cela ne signifie pas que vous êtes impuissant à les arrêter. Maintenant que vous savez ce que sont les logiciels malveillants et ce qu'ils peuvent faire, passons en revue les mesures pratiques que vous pouvez prendre pour vous protéger.

Comment prévenir les logiciels malveillants:

- Maintenez votre ordinateur et vos logiciels à jour
- Ne connectez pas de clés USB qui ne sont pas fiables.
- Utilisez Linux → pour une meilleure sécurité, les logiciels malveillants ne fonctionnant généralement que sous Windows.
- Réfléchissez à deux fois avant de cliquer sur des liens ou de télécharger quoi que ce soit

Phishing

Utilisé pour voler des informations, y compris des identifiants, des accès, des données. Il s'effectue principalement par le biais de courriels, de messages et d'appels téléphoniques.

Comment se défendre:

- Vérifiez que l'origine du message électronique est digne de confiance.
- S'il contient des adresses de sites web suspects.
- Si possible, vérifiez toujours la fiabilité du message auprès de la personne qui l'a envoyé.

“Attaque de l'homme du milieu”

Lorsque l'ennemi se connecte à nos réseaux, il peut espionner les informations qu'un appareil envoie via l'internet. Cette attaque peut être réalisée par des logiciels malveillants, à travers un réseau non sécurisé, par des agents sur le terrain et ainsi obtenir des informations sensibles.

Comment se protéger:

- Éviter les connexions WiFi celles qui ne sont pas protégées par un mot de passe.
- Prêter attention aux notifications du navigateur signalant qu'un site web n'est pas sécurisé.
- Se déconnecter immédiatement d'une application sécurisée lorsqu'elle n'est pas utilisée.
- Ne pas utiliser les réseaux wifi publics (par exemple, les cafés, les hôtels) pour effectuer des transactions sensibles.
- Utiliser un VPN.
- Utiliser TOR comme navigateur internet.

3. Cyber Attaque

Avec le développement de toutes ces technologies, il est devenu évident que les États utiliseraient ces outils et techniques pour attaquer, espionner et collecter des informations. D'autres États, comme les États-Unis, la Russie, l'Ukraine, Israël et l'Iran, se professionnalisent de plus en plus dans la réalisation d'attaques. L'OTAN mène de plus en plus d'attaques et de formations dans ce domaine.

L'exemple du logiciel malveillant Stuxnet en est un bon exemple. **Stuxnet est un ver informatique malveillant** découvert pour la première fois en 2010 et dont on pense qu'il est en cours de développement depuis au moins 2005. **Stuxnet cible les systèmes de contrôle des ordinateurs et des logiciels** et serait à l'origine de dommages considérables causés au programme nucléaire iranien. Bien que ni les États-Unis ni Israël n'aient ouvertement admis leur responsabilité, de nombreuses organisations de presse indépendantes affirment que Stuxnet est un ver informatique construit par les deux pays en collaboration. Stuxnet cible les machines utilisant le système d'exploitation et les réseaux Windows, puis recherche le logiciel Step7 de Siemens, qui est le programme utilisé dans le cadre du programme nucléaire. Stuxnet aurait compromis les systèmes de contrôle iraniens, recueillant des informations sur les systèmes industriels et provoquant la destruction des centrifugeuses à rotation rapide. Stuxnet aurait détruit près d'un cinquième des centrifugeuses nucléaires iraniennes. Ciblant les systèmes de contrôle industriels, le ver a infecté plus de 200 000 ordinateurs et provoqué la dégradation physique de 1 000 machines.

Ce n'est pas si loin de notre réalité. **La France a créé des logiciels malveillants pour espionner des fichiers, des informations, des lieux, notamment en Syrie.** Aujourd'hui encore, ce virus infecte des appareils et circule dans nos institutions. Le **malware Babar** en est un bon exemple, qui a été divulgué par le lanceur d'alerte Edward Snowden. Le logiciel espion Babar est capable d'enregistrer les frappes au clavier, d'enregistrer le presse-papiers, de faire des captures d'écran et même d'enregistrer les conversations audio sur Skype et Yahoo. Il peut injecter des codes dans des processus en cours d'exécution et voler des fichiers. Il utilise également le réseau Tor pour communiquer secrètement. Ce logiciel espion est certainement un outil d'espionnage et pourrait avoir été utilisé pour diverses raisons politiques.

La Turquie, malgré ses nombreuses faiblesses, a l'intention de devenir une puissance en matière d'attaques et d'espionnage numérique. En termes d'espionnage numérique, il existe actuellement une loi selon laquelle, pour que Google et Meta (Facebook, Whatsapp, Instagram) puissent opérer sur leur territoire, ces entreprises doivent fournir toutes les données qu'ils demandent, telles que la localisation, les messages, l'accès à leurs photos, etc. En particulier avant les attaques et les opérations de l'État, les médias numériques tels que Meta bloquent généralement les comptes qui partagent des contenus politiques, ce qui constitue une méthode de censure. **Par exemple, avant que les attaques de l'État turc contre le Rojava ne commencent à se produire, les comptes sur les plateformes de médias numériques comme Instagram, Twitter, etc. qui pourraient mobiliser contre ces attaques sont bloqués et fermés.**

Les capacités d'action des services de renseignement numérique sont principalement utilisées pour la surveillance intérieure et l'espionnage de leurs adversaires politiques, en utilisant les programmes de surveillance de puissances telles qu'Israël. En outre, l'espionnage des services téléphoniques dans d'autres pays tels que l'Arménie, la Grèce, Israël et la Syrie a déjà été prouvé. L'organisation de renseignement de l'État turc, le MIT, affirme également qu'elle travaille sur la sécurité numérique, les satellites et l'interception des signaux dans le monde entier.

Dans cette réalité, nous devons prendre conscience de notre utilisation des technologies, en particulier avec la spécialisation de notre ennemi, nous devons également nous professionnaliser, prendre conscience et nous préparer à une guerre qui est déjà devenue réelle. **Cette guerre doit suivre nos principes de guerre populaire révolutionnaire**, car une personne sans protection, une personne qui n'est pas prudente, peut mettre en danger des dizaines de camarades. Nous devons faire de ce sujet un thème commun à nous tous et à toute la société. **Nous devons tous travailler ensemble pour protéger nos identités, nos localisations, nos messages et nos informations.**

4. Sécurité des Caméras et des Microphones

Si l'ennemi veut prendre l'avantage sur vous par la surveillance des caméras et des microphones, il doit pirater votre appareil. Presque tous les piratages sont causés par des logiciels malveillants. **C'est en ouvrant des pièces jointes inconnues, en téléchargeant à partir de sources inconnues et en visitant des sites web non fiables qu'environ 98 % des logiciels malveillants** se retrouvent sur nos appareils. Une fois le logiciel malveillant installé, votre ordinateur ou votre téléphone est totalement accessible aux pirates. Il suffit d'éviter les logiciels malveillants et de s'assurer que votre logiciel antivirus est activé et à jour pour éviter cela.

Mais une fois le logiciel malveillant installé sur votre ordinateur, **l'ennemi peut accéder à votre microphone et à votre caméra.** La plupart des ordinateurs sont équipés de microphones et de caméras intégrés. Il en va de même pour les téléphones. Il est donc recommandé de couvrir toutes les caméras de vos appareils. Étant donné que les caméras et les microphones intégrés sont directement connectés à l'internet, ils sont très faciles à pirater. Dans ce cas, l'ennemi peut facilement prendre le contrôle de la fonctionnalité de la caméra et l'activer ou la désactiver à sa guise, ainsi que désactiver la lumière LED pour éviter d'être détecté. Bien entendu, il est également possible de bloquer toute autorisation et tout accès au microphone et à la caméra. Dans la plupart des cas, la protection logicielle est plus pratique que la protection physique, mais elle n'est pas toujours aussi fiable.

Il existe de nombreux logiciels permettant d'accéder à cette fonction. GrapheneOS, en particulier, offre cette option pour l'appareil dès le départ, ainsi que la possibilité de toujours vérifier si l'accès au microphone et à l'appareil photo est autorisé ou non.

Même si le fait de recouvrir votre caméra de ruban adhésif n'empêche pas quelqu'un d'écouter à travers le microphone, il s'agit d'une bonne protection de votre anonymat. Bien sûr, cela contrecarre la vidéosurveillance, mais le son du microphone peut toujours être capté. Les ordinateurs portables modernes sont souvent équipés de plusieurs micros pour améliorer la qualité du son, et il sera difficile de les filmer tous. Sur certains modèles, les microphones intégrés sont désactivés lorsque vous en connectez un externe. Une astuce consiste à brancher un mannequin dans la prise microphone (ou la prise universelle pour les micros et les casques). Votre ordinateur portable pensera qu'un micro externe est connecté et désactivera tous ses micros intégrés.

Dans la plupart des cas, la protection logicielle est plus pratique que la protection physique, mais elle n'est pas toujours aussi fiable. Nous devons toujours faire attention, lorsque nous parlons, à ne pas exposer d'informations à l'ennemi lorsque nous sommes à proximité de nos appareils.

5. Comment communiquer en toute sécurité

L'Application Signal

Pour communiquer en toute sécurité, il est bon de savoir si l'entreprise qui développe l'application du service de messagerie collabore avec la police, les États, si elle vend des données, etc. ou non.

Il existe plusieurs applications qui ne sont pas sécurisées, comme Whatsapp, mais certaines applications de communication offrent un cryptage. Bien sûr, avec le temps, de meilleures applications seront développées ou il est toujours possible que les applications utilisées soient prises en charge par l'ennemi. Par conséquent, il est généralement recommandé d'être prudent en matière de communication sur tous les appareils et de ne pas exposer d'informations sur ces plates-formes et applications.

Pour communiquer par messages/appels, l'application SIGNAL offre un très haut niveau de cryptage des communications contre les pirates informatiques. Elle est disponible sur tous les téléphones et également sur les ordinateurs. Il est possible de configurer des messages éphémères et plusieurs options pour plus de sécurité.

Comme nous l'avons mentionné précédemment, l'utilisation d'applications telles que Whatsapp n'est pas sûre, en plus de fournir des informations à des Etats comme la France ou la Turquie, Whatsapp a une sécurité très faible contre les attaques, il est très facile de découvrir des informations par le biais de technologies d'espionnage.

Un autre aspect très dangereux de Whatsapp est que tous les messages, même ceux qui ont été supprimés, sont stockés dans les fichiers Whatsapp. Si l'État turc demande vos messages, vos locations, vos numéros de téléphone, toutes vos informations seront transmises. Dans ce cas, même l'utilisation d'un VPN ne serait pas une solution complète, car seules vos informations seraient protégées, mais tous les messages et photos seraient toujours partagés, même plusieurs mois après leur envoi.

Tails

En outre, TAILS offre de nombreuses options de communication cryptée. De cette manière, de nombreuses communications peuvent être effectuées par les services qui sont disponibles sur TAILS. Cela peut améliorer notre vie privée en ligne.

Tails comprend:

- Tor Browser avec uBlock, un navigateur sécurisé et un bloqueur de publicité
- Thunderbird, pour des courriels cryptés
- KeePassXC, pour créer et stocker des mots de passe forts
- OnionShare, pour partager des fichiers, des sites web et des salons de discussion via Tor
- Metadata Cleaner, pour supprimer les métadonnées des fichiers

6. Bonnes pratiques à avoir

- Utilisez des mots de passe différents selon les comptes et les applications. La force d'un mot de passe est sa longueur, on parle même de phrase de passe pour plus de sécurité. L'utilisation de caractères spéciaux n'améliore plus la force d'un identifiant. Il est recommandé de concevoir un mot de passe de plusieurs mots aléatoires (un bon exemple serait “je pense raté ma sac à dos au moment de l’ouverture de ce bonbon habillé”, avec des espaces et des mots sans lien entre) pour un identifiant ou un ordinateur, et un mot de passe de 12 caractères pour un téléphone.

- Utilisez des applications sécurisées recommandées par vos camarades. Installez des applications provenant de sources fiables. Ces applications sont soumises à des contrôles de sécurité, ce qui réduit le risque d'activités malveillantes liées au microphone ou à d'autres fonctions sensibles.

- Ne répondez pas aux messages de contacts inconnus ou étranges et n'ouvrez pas les liens qui vous sont envoyés par ces derniers, car ils visent à obtenir votre position.

- Désactivez la localisation (GPS), la meilleure pratique étant de laisser votre téléphone portable toujours en mode avion. Le mode Wi-Fi peut être activé lorsque le mode avion fonctionne.

- Ne voyagez pas avec votre téléphone portable allumé. Si possible, retirez la carte Sim avant de vous rendre dans d'autres endroits, ce qui empêche également le déchiffrage de votre position par satellite.

- Organisez l'achat d'un emballage de sécurité qui coupe son signal (comme un sac de Faraday). Cet emballage empêche tout signal d'être émis par votre téléphone portable, ce qui en fait la meilleure option pour les voyages et les transports.

- N'envoyez pas de messages contenant votre nom, votre localisation, l'endroit où vous vous trouvez, l'endroit où vous allez. Les messages, en particulier sur Whatsapp, peuvent être interceptés et utilisés par les services de renseignement de l'ennemi.

- Utilisez une solution anti-virus et anti-malware. Il s'agit d'un logiciel ou d'un service essentiel qui protège les systèmes informatiques contre les logiciels malveillants. Ces programmes détectent les éventuelles menaces de logiciels malveillants, bloquent les menaces avant qu'elles n'accèdent au système et éliminent les menaces existantes afin qu'elles ne causent pas d'autres dommages au système. Pour cela, il existe plusieurs logiciels que vous pouvez télécharger sur vos appareils. Cela vaut pour tous les types d'appareils, comme les ordinateurs, les téléphones de tous les systèmes d'exploitation et même les téléphones équipés de GrapheneOS.

- Maintenez votre appareil à jour. Assurez-vous que votre appareil utilise le dernier système d'exploitation disponible et les derniers correctifs de sécurité. Les mises à jour régulières comprennent souvent des corrections de bogues et des améliorations de la sécurité qui permettent de remédier aux vulnérabilités potentielles. Ne pas mettre à jour pour assurer la sécurité est une idée reçue ou une fausse croyance. Il est préférable d'effectuer des mises à jour pour garantir la sécurité d'un appareil ayant un accès à l'internet.

Conclusion

Avec ce petit protocole de sécurité numérique, nous avons voulu partager avec vous quelques informations de base sur la manière de vous protéger au niveau numérique. Puisque les cyber-attaques augmentent et que l'utilisation des communications et des plateformes numériques devient de plus en plus présente, il est important que nous sachions comment les utiliser de manière sécurisée et comment rester protégés ou prévenir toute attaque de l'État ou d'autres ennemis à notre encontre. Puisque nous sommes la partie anticapitaliste de la société qui mène une lutte contre ce système, nous devons toujours nous rappeler que nous pouvons devenir la cible de telles attaques. Par conséquent, prendre notre sécurité au sérieux est une question très importante qui est essentielle pour nous tous dans la vie de tous les jours.

internationalistcommune.com