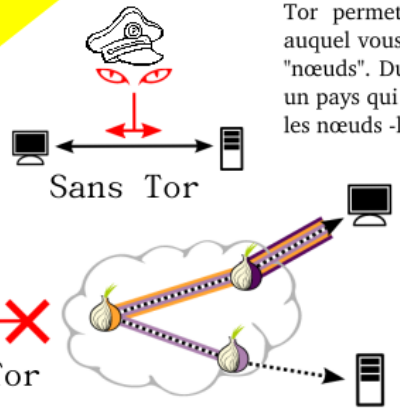


Tor permet également de contourner les censures. Le site auquel vous vous connectez ne connaît que le dernier des trois "nœuds". Du coup il suffit que ce dernier nœud soit situé dans un pays qui ne censure pas le site. (Il est possible de renouveler les nœuds -le circuit- jusqu'à obtenir l'accès au site voulu.)

Adresse I.P.?

IP : Internet Protocol. C'est le numéro par lequel un appareil est identifié sur le réseau. Ce numéro est attribué par le fournisseur d'accès internet/téléphone. Il sait donc à qui correspond l'adresse IP et doit conserver cette information pendant au moins un an pour pouvoir répondre à des requêtes judiciaires.

Profitez d'avoir instalé Tor pour vous **créer une messagerie sécurisée**! La solution la plus simple, c'est **Protonmail**. Les mails sont automatiquement chiffrés vers les autres utilisateur.rices de Proton, pour les autres, on détaille la petite manip dans la version en ligne de cet article!
Prenez-soin de choisir un **nouveau pseudo** auquel on ne pourra pas vous relier trop facilement.

Pour aller plus loin, vous pouvez utiliser **Riseup** qui est un hébergeur militant et vous renseigner sur la manière de crypter vos messages vous-mêmes, ce qui offre une meilleure protection (voir dans les liens).

Attention : seul le contenu des mails est chiffré, pas les objets ni les pièces jointes. Pour échanger des documents, mieux vaut passer par un intermédiaire comme Framadrop, et n'envoyer que l'adresse du lien dans le contenu du mail (chiffré lui).

Le système alternatif

Tails, c'est un système d'exploitation. Comme Mac, Windows ou Linux, sauf que vous ne l'installez pas directement sur l'ordinateur mais sur une clé Usb. (C'est ce que l'on appelle un sytème « live »).
Une fois l'installation effectuée sur la clé, vous la branchez simplement, et quand vous allumez l'ordinateur, il démarre sur Tails.
Vous vaquez à vos occupations, éteignez l'ordinateur, retirez la clé et redémarrez l'ordinateur : pour lui, il ne s'est rien passé. Vous pouvez redémarrer normalement sur votre système habituel, il n'en conservera pas de trace.
Logiquement, Tails fonctionne par défaut avec Tor (voir ci-dessus).
Ne rêvez pas, vous laisserez tout de même des traces sur internet, mais elles seront beaucoup plus difficiles à relier avec votre identité - et toujours à condition de rester vigilant.e sur vos activités, vos mots de passe, pseudos etc...
Tails contient tout un tas de logiciels qui le rendent très complet pour un usage courant (Suite bureautique, messagerie, navigateur web, logiciels de graphismes, traitement audio, montage vidéo, etc...), mais également de quoi nettoyer simplement les métadonnées (Mat) ainsi que le nécessaire pour aller plus loin dans la protection de sa vie privée et/ou de ses activités politiques.
Le site internet de Tails est vraiment bien fait et fournit pas mal d'explications : du téléchargement du fichier sur le site jusqu'à des réglages plus avancés ainsi qu'une présentation de chacun des logiciels fournis.

Tails
theamnesicincognitolivesystem

Le Guide d'autodéfense numérique : guide.boum.org/ — **Nothing To Hide** : frama.link/_SFDXBpX
Tor : nos-oignons.net - www.torproject.org/ — **Tails :** tails.boum.org/index.fr.html
Cryptage et mails : frama.link/mailchiffres - riseup.net/fr/security/message-security
Version complète de cet article : frama.link/GiletsLilleArticle

Guide (non-exhaustif) des bonnes pratiques face à la surveillance numérique

à 1'usage de Jojo avec son Gilet Jaune

Version complète de cet article :**https://frama.link/GiletsLilleArticle**

Nos téléphones, ordinateurs et internet de manière générale sont pratiquement incontournables dans nos luttes. Comme n'importe quels outils, ils sont à double-tranchant et peuvent s'avérer dangereux quand ils ne sont ni suffisamment connus, ni utilisés correctement.

Il ne s'agit pas ici de tomber dans la paranoïa, mais de simplement prendre conscience qu'on offre potentiellement beaucoup d'informations nous concernant en utilisant les outils numériques, et que ces infos peuvent être conservées très longtemps ensuite. Ce qui nous paraît anodin ou qui ne pose pas de problème de légalité aujourd'hui pourrait en poser demain.

Enfait, a première et peut-être la meilleure solution pour se protéger de la surveillance numérique serait de beaucoup moins, voir plus du tout utiliser son téléphone ou internet!

Si on souhaite quand même les utiliser, on peut au moins essayer d'adopter quelques bonnes pratiques.

Tous les outils que l'on propose sur cette page sont libres et gratuits. Libre au sens des « logiciels libres », c'est à dire que l'on peut avoir accès au code source du logiciel, le vérifier et l'améliorer.
Cela ne va pas être notre but ici... mais le fait que le logiciel puisse être vérifié par tous et toutes augmente la confiance que l'on peut lui accorder.

Enfin, renseignez vous sur les outils qu'on vous propose : les choses évoluent assez rapidement dans ce domaine. Les logiciels et applications nécessitent d'être mis à jour, de nouvelles menaces peuvent apparaître ainsi que de nouveaux outils pour s'en défendre.

Conseils de bases

- Ne publiez (ou mieux : ne prenez) jamais de photos qui pourraient incriminer quelqu'un ! Floutez systématiquement les visages des personnes et ne prenez pas de photos des personnes agissantes.
  Même en floutant les visages, les flics peuvent utiliser d'autres éléments, comme les vêtements, pour identifier des personnes
- Nettoyez les **métadonnées :**
  Essayez metadata.systemli.org et utilisez l'application Obscuracam qui permet de prendre des photos sans métadonnées et en floutant automatiquement les visages.

Métadonnées?

Quand vous prenez une photo avec un appareil ou un smartphone, le fichier que vous allez publier contient tout un tas d'informations, les métadonnées, qui concernent l'appareil que vous avez utilisé, la géolocalisation, l'heure ou l'ordinateur sur lequel vous avez retouché l'image et même potentiellement une version de l'image non retouchée…

- Utilisez Tor pour naviguer sur le web (on vous explique ça plus loin!)
- Ne donnez pas d'informations qui risquent de vous incriminer, vous ou quelqu'un d'autre par sms ou par mail.
- Faites attention à ne pas relier vos comptes à une adresse mail personnelle ou à votre numéro de téléphone qui vous identifient trop facilement.
- Utilisez des applications et des comptes sécurisés. (On reparle plus loin!)
- Attention à ce que vous publiez sur Facebook. La plupart du temps, votre compte est ouvert avec vos vrais noms et prénoms. Tout le monde y a accès, Facebook n'est pas particulièrement à cheval sur la protection de la vie privée - vraiment pas, puisqu'ils en font commerce - et n'hésitera pas à transmettre systématiquement vos informations à la Police.
  Par ailleurs, et ça c'est déjà vérifié, s'en remettre uniquement à Facebook pour s'organiser, c'est aussi prendre le risque de voir Facebook fermer la page ou le groupe…

Non, vraiment,
Facebook n'a pas de Gilet Jaune !

Le téléphone

Prendre son téléphone en manif, en action ou en réu, c'est pratique pour retrouver les ami.e.s mais si on se fait interpeller, on est susceptible de filer pas mal d'infos… **C'est dont prendre un risque pour soi et pour les autres.** Même sans se faire choper : il peut permettre de prouver que vous étiez bien présent.e à tel endroit à telle heure. Et l'éteindre ne suffit pas, la police peut utiliser ça comme un élément de suspicion à charge. Inversement s'il reste tranquillement allumé à la maison, ça peut laisser penser que vous aussi… À vous de voir !

Quand on reçoit des sms dont on se dit qu'ils pourraient poser des problèmes à la personne qui vous l'a relayé, mieux vaut les supprimer après avoir pris connaissance de l'info.
Attention à vos sms, c'est vraiment le type d'échange le moins sécurisé qui soit : Potentiellement, les flics sont capables de savoir exactement qui envoie quoi et à qui (ça ne veut pas dire qu'ils le font forcément tout le temps, ça veut dire qu'ils le peuvent).

Pour éviter qu'on puisse intercepter et lire vos messages, **utilisez et faites utiliser** les applications qui permettent de crypter vos messages tels que Signal et Silence!

Silence remplace votre application sms par défaut. Vous l'utilisez de la même manière sauf que les messages sont cryptés lorsque vous échangez avec un autre utilisateur de Silence.
Du coup, si les messages sont interceptés (ce qui est possible soit directement soit par demande au fournisseur d'accès téléphonique) on ne pourra pas en lire le contenu.
Et si vous ajoutez un mot de passe, on ne pourra pas lire vos messages en cas de perte ou de vol du téléphone.

Signal est un équivalent libre, sécurisé et chiffré d'applications comme Whatsapp', Telegram, etc.. (qui ne sont pas des applications libres). Cette application vous permet notamment de vous organiser en groupes de discussions et de diffusions sécurisés.
Comme pour Whatsapp' etc., il est nécessaire d'allumer les données de son téléphone pour l'envoi de messages sécurisés.
La principale différence, c'est que Signal est un logiciel libre et réellement gratuit, il ne gagne pas d'argent en collectant vos données.

Silence et Signal se ressemblent mais sont complémentaires et gagnent à être utilisées ensemble. Silence en messagerie sms par défaut, Signal pour gérer les messages multimédia, les conversations de groupe… Attention à ne pas désigner Signal comme application sms par défaut!

Un intérêt supplémentaire de Signal : si les flics font une requête auprès du fournisseur téléphonique, on ne pourra pas savoir avec qui vous avez échangé des messages ni quand (ce qui est possible avec des sms classiques et donc avec Silence). Ce genre d'information peut permettre de définir votre réseau social et potentiellement de voir des pics d'activités ou au contraire des baisses, pouvant sous-entendre une préparation d'action puis sa réalisation.

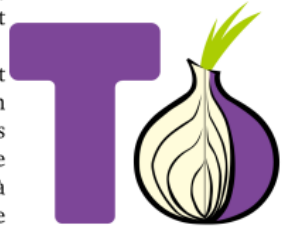
Pour que les échanges soient sécurisés et chiffrés de « bout en bout », il faut que les deux correspondant.e.s utilisent ces applications :

C'est pourquoi il faut les utiliser mais surtout les faire utiliser !

Naviguer sur internet

Pour vous rendre sur internet, vous utilisez un « navigateur », les plus courants sont Firefox (Mozilla), Google Chrome ou Internet Explorer (Edge).
Mais naviguer sur le web, c'est aussi (et surtout) laisser un certain nombre de traces, des données, qui font la joie et la fortune des « géants du web », notamment de Facebook et Google.
Ces informations concernent votre identité, votre localisation et vos activités en ligne mais peuvent aussi permettre à une personne mal-intentionnée, à un gouvernement et à sa police d'apprendre des tas de choses sur vous et vos proches, votre réseau et vos activités militantes… bref on gagnerait tous et toutes à se défendre un minimum contre ces curieu.ses.x.

Une alternative :
Le réseau Tor



Tor se présente lui aussi comme un navigateur, le Tor Browser, qui est une version modifiée Firefox et qui va vous permettre d'accéder aux pages web que vous voulez visiter par l'intermédiaire du réseau Tor.
Quand vous lancez le navigateur Tor Browser, il configure un circuit de trois "noeuds" qui sont autant d'intermédiaires entre votre ordinateur et la page que vous visitez.
Ces intermédiaires permettent d'éviter qu'une personne (un flic par exemple), en rouge sur l'image de la page suivante, ne puisse faire le lien entre les deux informations : vous (c'est à dire une adresse IP - et le site visité - ou ce que vous y publiez.