Manuel de sécurité informatique

Introduction

Ce document à pour objectif d'identifier quelles sont les menaces contre lesquelles l'organisation et ses militants doivent se prémunir, et de proposer des méthodes et outils concrets permettant de diminuer le risque que vous prenez dans le cadre de vos actions. Ce document essaye autant que possible d'appuyer ses dires sur des cas connus et documentés en source ouverte.
Les hypothèses et mesures proposées dans ce guide ne concernent que des activités menées dans le cadre de XR France. Si vous êtes membre d'une autre organisation, ou que vous avez des raisons de penser que vous faites l'objet d'une surveillance renforcée, ce document n'est peut être pas adapté à vous.
Quand on parle de sécurité, il y a plusieurs problématiques qui se cachent derrière, du coup on commence par quelques définitions.
L'anonymat : c'est la capacité de ne pas pouvoir relier vos activités en ligne avec votre identité réelle ou à un sous ensemble de données permettant de vous discriminer. Garantir son anonymat sur un forum vis à vis d'autres utilisateurs se limite juste à ne pas divulguer vos données personnelles. Par rapport aux administrateurs d'un forum ou de tout autre service informatique, il s'agira de masquer votre adresse IP (connexion en cybercafé, TOR, VPN). Par rapport à une régie publicitaire, il s'agira, en plus de masquer votre adresse IP, de berner l'ensemble des trackers qu'ils essayeront de vous imposer (cookies, images 1px, …).
La confidentialité des échanges : c'est le fait de maintenir secret des échanges, aussi bien le contenu lorsqu'il transit sur le réseau que le fait d'avoir ces échanges. Le secret des échange se basera généralement par du chiffrement de transport (SSL/TLS), alors que le masquage de l'activité réseau devra lui passer par la mise en œuvre de neouds rebonds (VPN ou TOR). La surveillance des échanges peut se faire au plus proche de chez vous (ex : les « boites noires » de la

loi renseignement) ou au plus proche des serveurs hébergeant l'activité (ex : piratage du serveur, mise sur écoute du datacenter par une autorité administrative ou judiciaire).
La confidentialité du stockage : c'est le fait de maintenir secret des données enregistrées sur un support de stockage. Là encore, on va parler de chiffrement, que ce soit de niveau système si on chiffre un disque entier ou de niveau fichier lorsque l'on utilise des outils type PGP/GPG. Le chiffrement en stockage vous évitera de vous faire voler les données auxquelles vous tenez (mots de passes, coordonnées bancaires, échanges perso, documents pro) si vous vous faites voler votre matériel.
Le chiffrement : c'est un mécanisme informatique, basé sur des propriétés mathématiques, qui permet de rendre illisible des données à qui n'a pas le secret ne permettant pas de les « décoder ». On parle de chiffrer pour l'opération rendant les données illisibles et de déchiffrement pour l'opération rendant les données à nouveau lisibles. On reversera le terme « décrypter » à une tentative de lire des données chiffrées sans disposer du secret nécessaire.

Il était une fois dans l'ouest

Les bons

Les touristes

Il s'agit des personnes qui souhaitent uniquement prendre de l'information afin de découvrir XR. Le principal objectif vis-à-vis d'eux est de ne pas être vecteur d'infection virale.

Activistes

Premier niveau d'engagement, l'activiste utilise pleinement les outils informatiques mis à disposition par XR.
Les actions XR se faisant à visage découvert, l'activiste n'a pas pour objectif de cacher son engagement, ce qui ne l'empêche pas de protéger sa vie privée. Afin de ne pas faire peser de risque sur les actions auquel il participe, il a la responsabilité de garder confidentielles les informations qui lui seront transmises par les organisateurs, dans les dernières phases de l'action. Si l'activiste soupsonne s'être fait voler des données, il doit prévenir les organisateurs des actions en cours afin que ceux-ci puissent s'adapter sans risquer de se retrouver nez à nez avec les FDO avant même d'avoir déroulé ses banderoles.

Organisateurs

Ils coordonnent tout ou partie des activités liées à une action.
Le niveau de menace à prendre en compte dépend de la nature de l'action organisée. Pour une action classique, le niveau de menace est moyen, il est peu probable que des moyens de renseignement soient mis en œuvre. Pour des actions plus risquées, le risque d'être assimilé à du terrorisme existe et des moyens de renseignement lourds peuvent alors être utilisés (voir plus bas).

Les brutes

Les brutes regroupent les acteurs qui sont en confrontation directe de l'organisation, que ce soit sur le terrain ou sur internet.

Le ministère de l'intérieur

Les objectifs du ministère de l'intérieur sont d'assurer le maintien de l'ordre, dont la sécurité des citoyens, le respect de la propriété privée et du droit de commercer et de lutter contre les actions terroristes ou qu'elle estime dangereuses pour la sécurité de la nation (cf. actions d'intrusion de Green Peace dans des centrales nucléaires ou le blocage de convois de déchets nucléaires).
Il dispose pour cela des FDO (police/gendarmerie, dont les unités spécialisées) et les services de renseignement. Les services de renseignement assurent une surveillance des organisations jugées à risque. XR peut être amenée à relever de cette catégorie selon la nature des actions effectuées. Ces moyens restent coûteux en ressources et en procédures, ils ne sont mis en œuvre que pour un petit nombre de personnes pour qui le niveau de suspicion est important.

- Objectifs : maintien de l'ordre, selon les choix politiques.
- Moyens :
  - Pendant une action
    - Ils peuvent mener une action d'infiltration.
    - Avec une fausse antenne relai (un IMSI catcher). Si vous avez un téléphone ("intelligent" ou non), il est possible d'identifier en temps réel l'identité des personnes présentes dans la zone à proximité (la centaine de mètres), et d'intercepter (écouter et modifier) les SMS et les appels téléphoniques. Cela ne permet pas d'intercepter le contenu de vos messageries utilisant internet, ni d'installer quoi que ce soit sur votre téléphone.
    - En cas de GAV, ils peuvent déverrouiller votre téléphone s'il est mal protégé, et aller voir toutes les données présentent sur le téléphone. Il est théoriquement possible de récupérer certaines des données non chiffrées qui ont été supprimés avant l'action, mais c'est peu probable que ce soit fait à moins de passer votre téléphone à un expert judiciaire.
  - En dehors d'une action
    - Perquisition et saisie de votre matériel informatique (ordinateurs, disques durs, téléphone). Ils peuvent lire tout le contenu qui n'est pas ou mal chiffré, récupérer une partie des données non chiffrées ayant été supprimées.
    - Requête judiciaire à votre opérateur de téléphonie mobile en vue d'obtenir les factures téléphoniques détaillées (appelées fadette). Elles permettent de connaître l'identité de vos correspondant.e.s de SMS et d'appels téléphoniques, et la localisation du téléphone (à l'aide des antennes relais). Elles ne contiennent pas le contenu des appels ou des SMS, mais ces méta données donnent énormément d'information pour savoir qui communique avec qui et corrélées avec d'autres infos comme la localisation, permettent d'en tirer beaucoup de sens. Ces données sont accessible pendant 1 an [ref de la loi qui les oblige à conserver ces données].
    - Requête judiciaire à vos fournisseurs de service en ligne coopérant avec les autorités françaises. Un utilisateur ordinaire d'un smartphone peut ainsi se voir reversé sans le savoir ses contacts, ses emails, son historique de navigation web, son historique d'itinéraires, son historique de position GPS s'il est identifié sur des comptes permettant une requête judiciaire.

  - Services de renseignements
    - Il est bien d'avoir en tête que dans le cas d'un collectif qui fait des réunions publiques, qui cherche à recruter de manière large, qui a beaucoup de primo-militant.e.s (qui n'ont donc pas une culture commune forte), il est extrêmement simple de s'inviter aux réunions et d'obtenir des renseignements ainsi, et que

protéger ses communications numériques ne permet pas du tout de s'en prévenir. Des récits d'infiltration de policiers.
    - Coopération avec l'opérateur mobile pour avoir en temps réel les informations de la localisation (à partir de la triangulation des antennes relaies), des destinataires de SMS ou d'appels
    - Usurper un certificat TLS (chiffrement https des pages web) sans lever de message d'erreur, et ainsi intercepter les mots de passes tapés dans un navigateur web, voir et modifier le contenu d'une page web telle que la messagerie Mattermost. C'est une attaque active qui peut être détectée ; il est avéré qu'elle a été "testée" en France mais pas dans un contexte réel d'interception, cela à par contre été utilisé en Iran, Libye et Tunisie sur des opposants politiques.
    - Accéder en temps réel aux sites visités depuis votre fournisseur d'accès internet. Cela permet de savoir que vous êtes sur le forum, mais pas sur quelle page en particulier (grâce au chiffrement https).

Il semblerait que la gendarmerie soit en train de développer sa capacité de récupération de données chiffrées et de déverrouillage de téléphones.

- Références :
    - Infiltration

https://iaata.info/Quelques-histoires-d-infiltrations-et-de-balances-en-Europe-depuis-quinze-ans-3548.html
https://www.lemonde.fr/pixels/article/2018/09/28/royaume-uni-les-services-secrets-anglais-avouent-avoir-illegalement-collecte-les-donnees-d-une-ong_5361676_4408996.html

    - Moyens

https://www.nextinpact.com/news/95934-la-loi-renseignement-publiee-au-journal-officiel-et-maintenant.htm
https://www.nextinpact.com/news/97700-loi-renseignement-liste-impressionnante-services-autorises-a-surveiller.htm
https://www.laquadrature.net/2018/12/13/cour-de-justice-de-lue-resume-de-nos-arguments-contre-la-surveillance-francaise/
https://www.nextinpact.com/news/108071-la-nouvelle-arme-anti-cryptographie-gendarmerie.htm

Les lobbies

Des grandes entreprises ou des lobbies assurent la surveillances des groupes activistes et ONG. Leur objectif est de maintenir leur position et de prévenir des actions négatives pour leur image de marque. Si on met ça sur le même plan que les méthodes d'espionnage industriel, tous les moyens sont bons: infiltration, désinformation (ternir l'image du mouvement), contre-information (green washing),... Les grands industriels ont recours, d'un côté à des officines de renseignement afin d'être prévenues en amont de potentielles actions, et de l'autre côté jouent de leur influence sur les pouvoirs publics et les politiques via les lobbies (cf procès de la cigarette aux USA, procès Servier en France, cash investigation sur les lobbies des emballages plastiques).

- Objectifs: limitation de la capacité de nuire, subversion, discrédit
- Moyens: vol de matériels, infiltration, renseignement, piratage
- Références :

https://www.greenpeace.fr/espace-presse/soupcons-despionnage-par-areva-greenpeace-porte-plainte/
https://www.amnesty.fr/actualites/le-pratiques-douteuses-ong

Les truands

Les truands sont les organisations qui relèvent surtout de l'espace médiatique. Leurs objectifs sont principalement de manipuler et de détourner le mouvement.

Le gouvernement/le monde politique

Son objectif principal est de se maintenir en place au fil des élections. Pris en tenaille entre une opinion publique qu'il cherche à flatter et des lobbies dont les objectifs ne sont pas forcément compatibles. Le gouvernement a bien évidement le contrôle du ministère de l'intérieur. Si le risque de l'employer en tant que police politique existe, il n'est pas clairement avéré dans notre cas.

- FIXME : Exemples .

Mouvements politiques et autres groupes et ONG

Les risques vis à vis de mouvements politiques, d'ONG ou d'autre mouvements sont une tentative de s'approprier ou de discréditer le mouvement. Cela peut être pour différentes raisons: intérêt politique, organisation "concurrente" prenant ombrage de l'action de XR (ex: autre ONG écologiste), organisation déçue ou rejetée suite à une convergence qui se passe mal.

- Exemples récents suite à la RIO : lettre ouverte des groupes de la convergence de l'action au centre commercial Italie 2.

Autres états

D'autres états peuvent être tentés de détourner le mouvement à leur profit afin de déstabiliser le gouvernement. La Russie est particulièrement active dans le domaine, sa stratégie de prédilection étant d'instiller le doute en diffusant de fausses informations (cf. élections américaines, françaises, campagnes de désinformation twitter/FB concernant les GJ, désinformation via les médias type Spoutnik/RT).

- Moyens: désinformation (ex : Spoutnik/RT), piratage (ex : élections américaines, Macron leaks), infiltration
- FIXME : Exemples

Opportunistes

On retrouve là toute une gamme d'acteurs qui ne cible pas spécifiquement XR, mais qui peuvent se servir des moyens mise en place pour les adhérents afin d'en tirer profit, types groupes mafieux diffusant des cryptolocker, récupération de données pour du phishing,...

- Moyens : vol de données, diffusion de malwares, piratage

Hygiène informatique de base :

Mesures de vigilance

Rester maître de ses données personnelles

Même si les actions XR se font à visage découvert, il est important de rester maître de ses données personnelles, sur internet en général mais également sur les outils XR. Ne donnez aucune information type nom/prénom/numéro de téléphone/adresse sur des moyens accessibles publiquement : canaux publics Mattermost, RDV 1&2, base hors messages personnels (attention aux messages personnels adressés à tout un groupe !). Assurez vous bien que seules les personnes ayant besoin de ces infos puissent les avoir, en particulier les coordinateurs.

Rester méfiant avec les e-mails

Restez toujours vigilants vis à vis des mails que vous recevez. Lorsque vous recevez un mail avec une p.j. ou vous demandant de suivre un lien, posez vous au moins deux questions :
Est-ce que le mail viens bien d'une personne que je connais ? (attention, il arrive aussi que des proches se fassent pirater leurs compte mail et que ce dernier soit utilisé en rebond)
Si il s'agit d'un mail provenant d'une entreprise ou de l'administration, y-a-t'il quelque chose de louche ? Il peut s'agir d'une adresse mail source bizarre, une charte graphique inhabituelle, des fautes d'orthographes, des demandes atypiques ou des adresses web très proches mais différentes de l'adresse normale de l'entreprise. Gardez en tête qu'une entreprise légitime ne vous demandera jamais un mot de passe ni un numéro de carte bleu. Elle vous enjoindra en général à vous connecter à ses services, sans fournir un lien dans le corps du mail.

Ne pas se connecter aux réseaux wifi ouverts (ou avec un VPN)

Les réseaux wifi ouverts posent de nombreux problèmes. Ils créent l'opportunité de créer de faux points d'accès wifi qui vont voler vos identifiants, peuvent écouter le trafic que vous générez, peuvent permettre aux autres personnes connectées au même point d'accès de tenter de vous pirater… Pour éviter ça, le mieux est simplement de ne pas s'y connecter ! Si vous disposez d'un smartphone et d'un forfait avec suffisamment de datas, le mieux est de se connecter à internet via ce dernier (par USB ou point d'accès wifi dédié). Si ce n'est pas possible (à l'étranger, pas de smartphone ou de forfait) et que vous n'avez pas d'autre moyen, il faut mettre en œuvre un tunnel VPN.
L'utilisation d'un VPN doit toutefois être faite avec discernement. Toutes les communications que vous faites passent par un lien chiffré entre vous et votre fournisseur d'accès VPN. Si un VPN vous protégera bien en cas d'interception au niveau de votre fournisseur d'accès (que ce soit un FAI ou le wifi de l'hôtel), il reportera le problème sur le fournisseur d'accès VPN qui aura alors toutes vos données de connections, ce qui signifie qu'il vous faudra avoir une confiance importante dans votre fournisseur d'accès VPN. Et là, tous les fournisseurs ne sont pas égaux. On risque de se retrouver à fournir ses données à des entreprises (ou états) peu scrupuleuses alors qu'en plus on a payé pour ce service. Pour y voir plus clair et vous aider dans vos choix, vous pouvez vous aider de comparateurs tels que https://thatoneprivacysite.net/#detailed-vpn-comparison.

- Références :

https://www.computerweekly.com/news/252466203/Top-VPNs-secretly-owned-by-Chinese-firms
https://www.techdirt.com/articles/20190122/10263541441/study-again-finds-that-most-vpns-are-shady-as-hell.shtml

https://www.theregister.co.uk/2017/08/07/hotspot_shield_deceives_with_false_privacy_promises_complaint_claims/

Mesures techniques

Mises à jour/anti-virus/firewall (ordinateur)

Il faut avoir un système récent soutenu par son éditeur. La mise à jour est activée par défaut sur les version récentes, ne pas désactiver. De même, les principaux logiciels doivent être maintenus à jour, dont en premier lieu le navigateur web.
Avoir un OS à jour permet de se prémunir des vulnérabilités publiées, qui sont utilisée dans les malwares communs.

Sous Windows, il faut avoir un anti-virus et un pare-feu activé. Ceux fournis par défaut par Microsoft (Windows Security et parfeu système) font le job.
Référence : https://www.lemondeinformatique.fr/actualites/lire-faut-il-arreter-d-acheter-un-antivirus-76586.html

Installer des bloqueurs de publicités et de trackers (tous périphériques)
Les bloqueurs de publicité allégent les pages web et évite de se faire profiler par les distributeurs de publicité. Deux approches sont possibles :
1/ Utiliser un module navigateur : Firefox + uBlock origin + Decentraleyes
Cette solution est plus simple à mettre en œuvre, mais ne fonctionne que sur les navigateur web.
2/ Utiliser une liste d'hôtes à bloquer :
Cette solution est plus complexe à mettre en œuvre, mais permet de prendre en compte les trackers quelque soit l'application (dont les publicités dans les applications mobiles).
Vous trouverez d'avantage d'informations sur la manière de procéder et une liste prête à l'emploi à l'adresse suivante : https://sebsauvage.net/wiki/doku.php?id=dns-blocklist

Mots de passe complexe et gestionnaire de mot de passe
Afin d'éviter de se faire voler ses comptes en ligne, il est conseillé d'utiliser des mots de passes complexes (>10 caractères avec minuscules/majuscules/chiffres/caractères spéciaux) et différents pour chaque site. Et comme ça deviens rapidement ingérable, il est conseillé d'utiliser un gestionnaire de mot de passe, permettant de générer et stocker de manière sécurisée tous vos mots de passe. Des modules permettent de s'intégrer dans les navigateurs afin de compléter automatiquement les champs.
En local : keepass, simple et robuste mais ne permet pas nativement la synchronisation entre différents périphériques. Vous pouvez toutefois retrouver cette capacité en couplant l'outil à des services de stockage dans le cloud (dropbox, google drive, OneDrive,…).
Avec synchronisation en ligne (permet le partage automatique entre différents périphériques) : Firefox LockWise (intégré de base dans la fonction sync de Firefox), bitwarden

En complément des mots de passe, il faut vraiment s'astreindre à activer l'authentification à deux facteurs pour les services qui le proposent, en particulier pour les services mails. Même si cette solution est contraignante et imparfaite, le niveau de sécurité est alors bien supérieur.

- Références :

https://n.survol.fr/n/developpeurs-vous-devriez-avoir-honte-regles-de-mots-de-passe

https://n.survol.fr/n/dis-tonton-comment-ca-fonctionne-la-securite-dun-gestionnaire-de-mots-de-passe-introduction-cryptographique

Sauvegarder ses données personnelles

Il est important de réaliser des sauvegardes de ses données. La perte de vos données peut avoir de nombreuses raisons : incendie, dégât des eaux, vol (à la maison ou en déplacement), perquisition,...
Sauvegarder chez soit, c'est bien, mais, vu les raisons évoquées ci-dessus, sauvegarder en ligne, c'est mieux. Mais d'un autre côté, vous n'avez pas non plus envie de confier vos données à n'importe qui, du coup il va falloir les chiffrer avant de les transmettre au service de sauvegarde. Duplicati vous permet de venir en surcouche de nombreux fournisseurs de stockage cloud et apporte des fonctionnalités de backup incrémental. Pour le service de stockage en lui même, cela dépend du volume de données à sauvegarder. Les offres gratuites suffisent pour de petits volumes (<5/10Go), mais si vous avez besoin de plus gros volumes (ex : base des photos familiales des 10 dernières années...), il vous faudra sans doute passer par un service payant, comme peuvent le proposer Jottacloud ou pcloud.
De manière générale toute donnée que vous ne sauvegardez pas peut être perdue du jour au lendemain. Posez vous bien la question pour toutes vos données (photos, cv, documents rédigées,...).
Considérez que toute donnée stockée sur un service en ligne, à plus forte raison par une grande entreprise d'internet (google, MS, dropbox,...), sans avoir été préalablement chiffrée est potentiellement visible par n'importe qui. Si ces données ont une quelconque valeur pour vous ou votre entreprise, chiffrez, chiffrez, chiffrez...

Chiffrer ses données

Le chiffrement de disque permet de garder vos données confidentielles dans le cas ou vos périphériques sont volés. Le chiffrement ne vous protégera par contre pas en cas de perquisition, car un jeu peu vous ordonner de donner vos mots de passe (et y contrevenir vous coûtera très cher, voir le post suivant sur la base : https://base.extinctionrebellion.fr/t/comment-proteger-verouiller-son-telephone/30200/8).
Si vous n'avez pas de gros besoins de performances (jeux vidéos récents, montage video,...), vous pouvez utiliser Veracrypt (https://www.veracrypt.fr/) pour chiffrer vos partition systèmes ou créer des conteneurs chiffrés. Si vous chiffrez vos partitions systèmes, il est très important de correctement générer une clef USB de sauvetage. Cette dernière vous permet de déchiffrer le disque (avec le mot de passe bien sur) si jamais votre système d'exploitation venat à ne plus fonctionner. Cela vous permettrai alors de pouvoir récupérer vos données ou de réparer le système.
Sinon vous pouvez vous limiter à l'utilisation de conteneurs sécurisés, toujours avec Veracrypt, qui apparaîtront comme des disques durs supplémentaires et dans lesquels vous pourrez placer vos données d'interet. Attention toutefois à ne pas créer des conteneurs trop gros, au risque d'avoir des problèmes avec les outils de sauvegarde.

Hygiène spécifique aux activités XR

L'idée générale est de séparer ses activités militantes de ses activités usuelles pour éviter de des liens trop évidents puissent être faits.

Utilisation d'un compte mail dédié

Le compte mail est la pierre angulaire de la sécurité de vos comptes en ligne. Il permet pour la quasi totalité des services de réinitialiser vos mots de passe. Il est donc particulièrement important d'utiliser une authentification à deux facteurs (SMS, authentificateur, token USB) pour l'accès à votre boite mail. Un des risques lié aux boites mail est la transmission de vos données à un état (français ou autre) par le fournisseur du service. Il est alors important de bien choisir son fournisseur afin d'avoir suffisamment confiance. Certains services mettent en avant le fait de résider dans les pays où les lois relatives à la vie privée sont particulièrement strictes, d'autre mettent en avant des mesures techniques et de non journalisation des données.
Fournisseurs possibles : protonmail (hébergement en Suisse, offre de base gratuite), posteo (hébergement « green » et garantie d'anonymat, offre de base 1€/mois).

Échanger via des canaux sécurisés

Échanger des messages

Mattermost et la base sont des moyens de communication publics. Il faut les considérer comme tels et se dire que tout ce qui y est dit est lisible pas les RG. Afin de pouvoir échanger de manière confidentielle, il vaut mieux utiliser des messageries comme Signal, Matrix/Riot ou Wire. Signal à l'avantage de ne pas nécessiter d'infrastructure dédiée, mais en contrepartie nécessite de donner son numéro de téléphone pour pouvoir être retrouvé. A l'inverse, Matrix/Riot permet de gagner en anonymité, mais nécessite d'héberger un service commun sur internet (possibilité de mettre en œuvre un tel service au sein de XR ?). Wire ne nécessite pas de numéro de téléphone pour se créer un compte et propose également un haut niveau de sécurisation des communications.
Vous trouverez un comparatif des différents outils de messagerie instantanée à cette adresse : https://www.securemessagingapps.com/.

Échanger des données/fichiers

Pour partager des fichiers de manière sécurisée (i.e. : non lisible par un tiers, par l'hébergeur, ou par une personne ayant volé votre matériel), il faut une fois de plus recourir à du chiffrement de bout en bout.
La solution la plus simple est probablement d'échanger des fichiers entre boites mails protonmail. Entre les boites, les messages sont chiffrés par OpenPGP de manière transparente.
L'excellent 7-zip (http://www.7-zip.org/) permet aussi de faire ça très facilement si tout le monde n'a pas de boite mail chez proton. Il suffit de compresser les fichiers avec un mot de passe. Ce mot de passe devra toute de même être robuste (>10 caractères – lettres, chiffres, signes) qui devra alors être communiqué aux destinataires via un canal différent de celui du mail (c.f. options ci-dessus, par signal par exemple).
Il existe des solutions pour poster un texte en ligne (non modifiable)+fil de discussion (PrivateBin https://privatebin.info/) ou de bureautique plus classique (https://cryptpad.fr/), qui permettent de partager des données de manière chiffrée. Les opérations de chiffrement/déchiffrement étant réalisées du côté des clients web (vous donc), ni l'hébergeur ni un autre client ne peut accéder aux données sans avoir également la clef de déchiffrement. En revanche, l'hébergeur n'ayant pas connaissance des activités sur son serveur prend le risque que des utilisateurs aient un usage illégal du service.
Attention, si vous utilisez certains de ces outils, le mot de passe de déchiffrement est contenu dans l'adresse du document. Cette adresse doit donc être transmise via un moyen également

sécurisé et être jalousement gardée (dans un gestionnaire de mots de passes ou dans une boite aux lettres protonmail par exemple).

On retrouve également parmi les solutions les mails chiffrés avec PGP/OpenGPG (hors proton qui l'embarque quant à lui de manière transparente), que l'on peut mettre en œuvre avec protonmail (en ajoutant manuellement les clefs des destinataires hors proton), le client mail Thunderbird et l'extension Enigmail ou Firefox avec l'extension mailvelope pour une utilisation en mode webmail (sauf que mailvelope ne fonctionne pas avec le navigateur TOR…). Ces outils ne sont toutefois pas évidents à mettre en œuvre et nécessitent d'en comprendre un minimum les principes.

Utilisation d'une session spécifique

Simple et pas cher, utiliser un compte utilisateur sans droits administrateur permet de séparer vos activités. Notamment, les outils de tracking auront plus de difficultés, en complément de l'utilisation de TOR, à faire le lien avec vos activités habituelles.
En cas d'infection virale type cryptolocker (ex : fichier sur le cloud XR, mail piégé), cette mesure pourra (selon la nature du malware) limiter la propagation à l'ensemble des données.

Utilisation de TOR Browser

L'objectif de TOR est double. D'un côté, il permet d'empêcher un attaquant écoutant vos communication d'avoir connaissance des sites web visités. De l'autre côté il permet d'empêcher le serveur auquel vous vous connectez de connaître votre adresse IP (ce qui n'interdit pas l'identification par d'autres moyens, dont adresse mail donnée pour créer un compte qui doit donc être spécifique à ce service ou à un ensemble cohérent). L'inconvénient de TOR est en revanche qu'il ralenti la navigation et que son navigateur peut être un peu spartiate.

Pour le mettre en œuvre il est indispensable d'utiliser une version de TOR intégrée dans un navigateur spécifique proposé par le site http://www.torproject.org. Les solutions à base de modules ou de box réseau sont déconseillées car elles ne permettent pas de maîtriser certains flux annexes dont les requêtes DNS.

Et le téléphone dans tout ça ?

Jusqu'ici, il les propositions portent surtout sur des ordinateurs. Au sujet des smartphones, un guide concernant leur verrouillage lors des actions existe sur la base :
https://base.extinctionrebellion.fr/t/comment-proteger-verouiller-son-telephone/30200

Pour aller plus loin

Une page dédiée sur la base recense des pointeurs vers des formations plus complètes :
https://base.extinctionrebellion.fr/t/ressources-externes-de-formation-a-lhygiene-securite-numerique/25846.
Vous trouverez ici quelques références (complémentaires ou reprises du post) pour ceux qui souhaiterai approfondir leurs connaissances. Le post étant en wiki, n'hésitez pas

La fondation Mozilla à publié un billet sur son blog sur le sujet de l'hygiène informatique : https://blog.mozilla.org/firefox/fr/comment-proteger-son-identite-en-ligne/ . Il couvre la majorité des aspects, que nous compléterons ici avec des suggestions d'outils.
Pour ceux qui souhaitent creuser les notions de sécurité informatique, une autoformation est disponible sur le site suivant: https://www.secnumacademie.gouv.fr/
L'association nothing2hide travail également à la sensibilisation d'acteurs associatifs et de journalistes. De la documentation et des supports de formation (un peu arides toutefois sans bande son) sont en ligne sur https://nothing2hide.org/fr/ . A noter notamment la formation sur le volet analyse de la menace/analyse de risque qui met bien en avant le fait que la sécurité absolue n'existe pas mais qu'une approche pragmatique qui vise à identifier contre quoi se prémunir peut être mise en œuvre.
A noter également, pour avoir une compréhension plus claire de ce que sont HTTPS, TOR et les VPN d'un point de vue technique et dans le cadre du respect de la vie privée, l'article https://linuxfr.org/news/https-tor-vpn-de-quoi-est-ce-que-ca-protege-exactement vous éclairera sur ces sujets.

Enfin, cette page wiki recense une quantité importante d'informations en tout genre autour de la sécurité informatique. Ce n'est pas forcément très accessible de prime abord, mais c'est très riche : https://groupes.renater.fr/wiki/cryptobib/