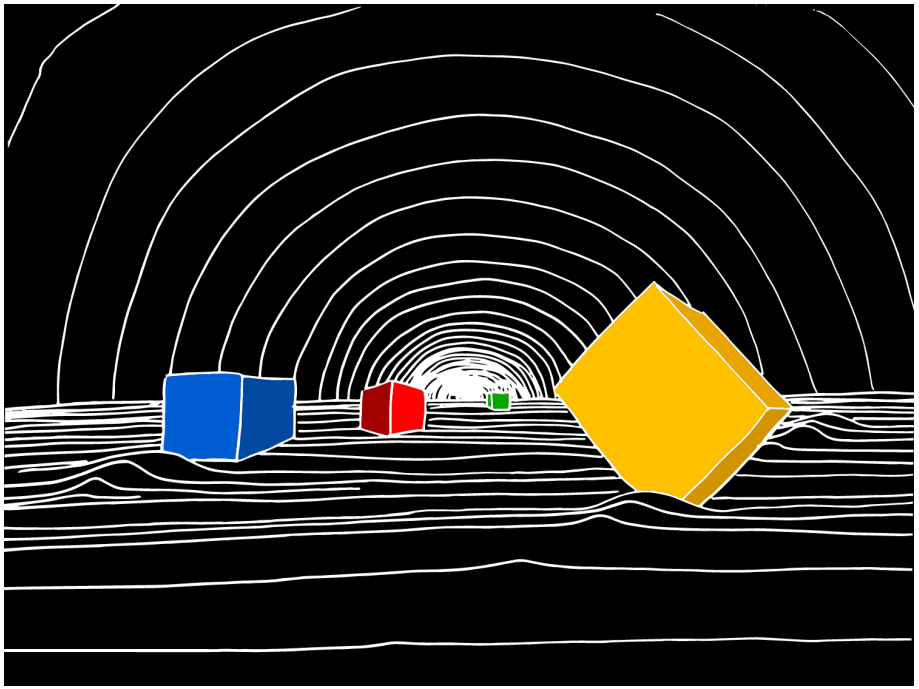
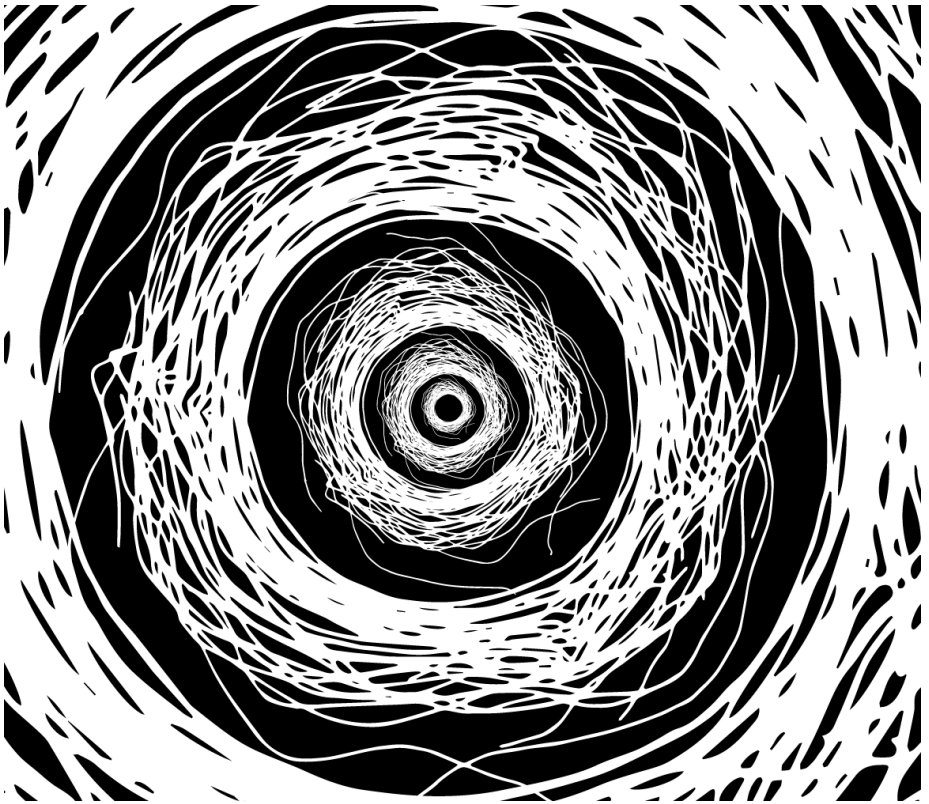
Quelles sont les principales menaces numériques et comment s'en protéger ? Comment fonctionne la surveillance numérique ? Que penser de Signal ? Des mails ? Des smartphones ? Comment gérer ses mots de passes ? Que faire des réseaux sociaux ? Ce guide de survie tente de présenter de manière synthétique des éléments de réponses à toutes ces questions.



Boîte à outils de la Zad du Carnet

Guide de survie numérique à l'usage des militant·es



Guide élaboré sur la Zad du Carnet en 2020/2021 et mis à jour en juin 2024
Pour toutes remarques, contactez guidesurvienum@riseup.net

La diversité des tactiques existe aussi dans la protection numérique

Utiliser des outils numériques n'est pas quelque chose d'anodin. Ne pas laisser de traces, de potentielles preuves sur son téléphone ou ordinateur est une mission impossible. Utiliser des smartphones ou ordinateurs quand on connaît les conditions de travail des ouvriers et ouvrières de la chaîne de production de ces objets numériques est un reniement de nos valeurs anticapitalistes.

Pourtant le terrain d'Internet et du numérique est un lieu de lutte important et le déserter totalement serait une erreur. Mener de front la lutte pour se libérer de notre dépendance aux outils numériques tout en se formant à mieux les utiliser pour lutter efficacement via ces outils peut paraître incohérent. Ce n'est pourtant qu'un aspect de la diversité des tactiques. Il est important de comprendre, de tolérer et de s'entre-aider entre personnes faisant le choix d'utiliser le moins possible les outils numériques et personnes faisant d'Internet leur principal lieu de lutte. Ces deux méthodes de lutte sont complémentaires.

Ce guide est destiné aux personnes utilisant quelques fois des outils numériques (téléphones, ordinateurs, etc.) dans leur militantisme. Il expose quelques menaces et présente des contre-mesures partielles pouvant aider à protéger contre ces menaces.

Il est important de noter que la lutte pour la sécurité informatique est une question de ressources disponibles. Des attaquants puissants avec du temps devant eux pourront toujours contourner les méthodes de protection que l'on met en place. Les mesures de protection que l'on conseille dans ce guide ne sont donc jamais parfaites.

Pour déterminer quelles mesures de protection sont adaptées à une personne ou un collectif, on pense souvent d'abord aux menaces dont iels pourraient être les cibles. Ainsi on trie les menaces par ordre de probabilité et gravité selon nos activités pour se protéger en priorité des plus probables. C'est l'approche de la sécurité numérique par modèle de menaces.

Les modèles de menace doivent être envisagés dans un cadre collectif. En effet la sécurité numérique est un ***enjeu collectif et non individuel*** *: en se protégeant, on protège les autres autour de nous et quand les autres se protègent, iels nous protègent aussi.*

8. Ressources utiles

- https://tails.boum.org/home/index.fr.html Le site de Tails pour installer Tails et apprendre à l'utiliser. Ce site regroupe également beaucoup de documentation.
- Comment se protéger et protéger nos luttes, brochure sur infokiosques.net
- Le TuTORiel Tails disponible sur infokiosques regroupe de nombreux tutoriels.
- https://guide.boum.org/ Les tomes 1 et 2 du guide d'autodéfense numérique sont des références.
- https://riseup.net/en/security Le site de Riseup regroupe de nombreux tutoriels
- https://fr.vpnmentor.com/blog/la-plupart-des-lgbtq-se-font-harceler-en-ligne-voici-comment-rester-en-securite/ regroupe de nombreux conseils à destination des LGBTQI+ pour éviter le harcèlement en ligne
- https://securityinabox.org/en/ regroupe de nombreux tutoriels en anglais et possède une version francaise : https://securityinabox.org/fr/
- Le projet évasion propose plusieurs textes en téléchargement : l'excellent « Comment la police interroge et comment s'en défendre » ainsi que le Guide de sécurité digitale à l'usage des travailleureuses du sexe : projet-evasions.org/
- Le site de la quadrature du net mène diverses actions contre la surveillance et écrit des articles sur l'actualité https://www.laquadrature.net/
- Le Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires (CHATONS) propose des services libres et décentralisés comme par exemple l'hébergement d'adresse mails chatons.org/. Riseup recense sur son site une liste de serveurs politiquement engagé à travers le monde pour des services libres et décentralisés : riseup.net/en/security/resources/radical-servers
- Le No trace project regroupe des outils pour contrer la surveillance : www.notrace.how/fr/

Crédits des images dans l'ordre (numéro de page entre parenthèses)

1. Image de la quadrature du net (1)
2. Représentation de la triade CIA par Ljean (2)
3. Capture d'écran du logiciel KeepassXC (7)
4. Tableau inspiré d'un article Wikipédia (8)
5. Image de la brochure Téléphonie mobile (11)
6. Logo de Technopolice.fr CC-BY-SA 4.0 (13)
7. Logo de Linux Unified Key Setup (20)
8. Image du guide d'autodéfense numérique(Tor, 23)
9. Image du guide d'autodéfense numérique (PGP, 27)
10. Logo de XMPP (30)
11. Logo de Tails (33)
12. Image de la quadrature du net (40)

7.2. Pour les téléphones

Atelier 1 : changer les paramètres de confidentialité de toutes ses applications et supprimer celles que l'on utilise pas. Enlever également toutes les notifications sur l'écran de verrouillage.
Durée estimée : 3h

Atelier 2 : Installer des applications plus respectueuses de la vie privée.
Durée variable
On pense à Organic maps, F-droid, Orbot, Conversations, Signal, Tor Browser, Firefox, NewPipe etc.

Atelier 3 : Chiffrer son ou ses smartphones
Durée estimée : 2h
Les techniques de chiffrement sont variables selon les systèmes d'exploitations et cela est impossible pour certains systèmes d'exploitation.

Atelier 4 : acheter un téléphone cash et une carte SIM prépayée anonyme (Lycamobile, Lebara, Syma, etc.) pour un usage militant.
Durée estimée : 3 heures (recherche sur les sites d'occasion et achat cash).

7.3. Autres ateliers

Atelier 1 : Mettre en place un lecteur de flux RSS
Durée estimée : 2h

Atelier 2 : Mettre des gommettes sur les caméras des ordinateurs et téléphones que l'on utilise.
Durée estimée : 30 minutes (achat des gommettes et mise en place)

Atelier 3 : Si l'on utilise les réseaux sociaux pour publier du contenu militant, créer un site web et apprendre à manier l'administration du site.
Durée estimée : variable, compter 1 journée entière

Atelier 4 : Apprendre à publier du contenu sur les réseaux Mutu
Durée estimée : 1h
Le langage SPIP est facile à apprendre et l'interface des réseaux Mutu est facile à maîtriser.

Atelier 5 : Transmettez ce que vous avez appris à d'autres militant·es
Durée estimée : longue
Se protéger seul·e est loin d'être suffisant car la protection numérique est un enjeu collectif, il est important de diffuser les savoirs.

Table des matières

Plan du document

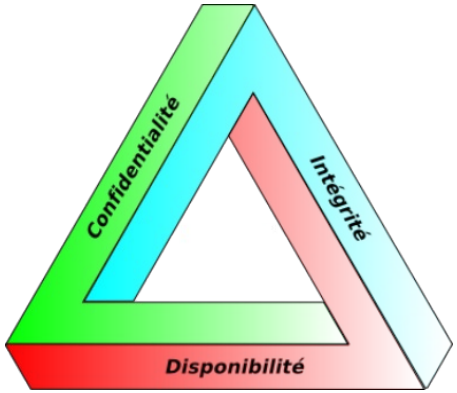
On parlera dans ce guide d'attaques pour obtenir des données numériques que l'on souhaiterait garder privées. On présentera d'abord les attaques les plus courantes, celles liées aux erreurs humaines. On parlera ensuite des attaques spécifiques aux supports physiques que l'on utilise : téléphone et ordinateur. Nous finirons par les attaques spécifiques à l'utilisation d'Internet, plus précisément à la navigation web, à la messagerie instantanée et aux mails.

Il va sans dire que si vous utilisez un téléphone portable pour consulter une messagerie instantanée, vous pouvez subir des attaques spécifiques aux téléphones ainsi que des attaques spécifiques à la messagerie instantanée.

Pour chaque attaque, nous présenterons des méthodes pour se protéger. Ces méthodes ne seront pas toujours elles mêmes fiables mais peuvent améliorer vos défenses face à un attaquant. Mettre en place une mesure de protection numérique de manière efficace, c'est comprendre en quoi elle nous protège d'une certaine attaque mais aussi de ses limites face à d'autres types d'attaques.

Avec ces mesures de protection, on souhaite complexifier le fichage, éviter la récupération de données en cas de perquisitions et éviter de fournir des preuves judiciaires. Viser l'anonymat total serait beaucoup trop ambitieux. Ce guide n'est qu'un guide de survie, il ne présente que quelques attaques potentielles et quelques contre-mesures et est loin d'être exhaustif.

Pour les personnes pressées, on pourra lire uniquement les conseils de la dernière section « En pratique, que faire ? » qui répète les principales méthodes de protection de la brochure.



Quand on parle de sécurité numérique, on cherche à préserver la confidentialité, l'intégrité et la disponibilité de nos données

7.1. Pour les ordinateurs

Atelier 1 : trier ses données et faire une sauvegarde sur un disque dur (non chiffré) de l'intégralité de ses données.
Durée estimée : variable, compter 3-4h minimum (le temps de copie des données peut être long).

Atelier 2 : Créer une clé Tails, l'apprivoiser et configurer le stockage persistent.
Durée estimée : 2h.

Atelier 3 : Créer des mots de passe robustes via Diceware et les mémoriser

Durée estimée : 1h

Chercher une liste de mots Diceware sur Internet et tirer des dés 6. Pour mémoriser les mots de passe, on pourra les noter temporairement sur un bout de papier (pour ne pas les oublier) et essayer de les utiliser régulièrement.

Atelier 4 : Installer un gestionnaire de mots de passes, changer ses mots de passes pour de nouveaux mots de passe uniques et mettre en place une base de données de mots de passe.
Durée estimée : 3h
On fera attention à copier la base de données de mots de passe sur de multiples supports : clé Tails, disque dur de sauvegarde, ordinateur personnel, etc. On conseille de choisir un nouveau mot de passe unique particulièrement robuste (par exemple via la méthode Diceware) pour la base de données qu'on oubliera pas sous peine de perdre l'intégralité de ses mots de passe. Notez que vous devrez avoir accès à votre base de données pour accéder à des services nécessitant des mots de passes vu que vous ne les connaîtrez pas par coeur.

Atelier 5 : Créer une clé Tails de sauvegarde.
Durée estimée : 1h

Atelier 6 : Créer de nouvelles adresses mails pour compartimenter les usages
Durée estimée : 1-3h
On préfèrera créer des adresses sur des serveurs mails variés dans une optique de décentralisation (voir la liste de serveurs radicaux par Riseup cité plus haut)

Atelier 7 : Utiliser le protocole PGP pour toutes ses adresses mails
Durée estimée : 3h

Atelier 8 : Créer un disque dur de sauvegarde chiffré.
Durée estimée : variable, compter 4h (temps de copie des données peut être long).

6.7. Bien gérer ses mots de passe et options de confidentialité

Si cela n'est pas déjà fait, on peut choisir un nouveau mot de passe fort pour créer une base de données de mots de passe et tendre vers le fait d'avoir des mots de passe uniques pour chaque service que l'on utilise.

On conseille de mettre au maximum les options de confidentialité des applications que l'on utilise et installer des modules supplémentaires de protection de la vie privée. Sur Firefox, on recommande d'activer le mode https uniquement et d'utiliser les extensions suivantes : Privacy Badger, Ublock Origin, Cookie Autodelete.

6.8. Limiter notre dépendance aux plateformes capitalistes et encourager les alternatives

Les outils numériques sont cernés par les géants du capitalisme. Cette brochure s'adresse principalement à des militant.es pour qui l'anticapitalisme est une évidence et on ne reviendra en détails pas sur les raisons de s'opposer aux multinationales capitalistes.

Pour soutenir les luttes contre ces géants destructeurs, essayons au maximum de limiter notre dépendance à eux et de nous émanciper d'eux et à les attaquer. Plus précisément, on pense aux

- GAFAM (Google, Amazon, Facebook, Apple, Microsoft)
- réseaux sociaux centralisés (Instagram, Twitter, Facebook, Snapchat, etc.),
- etc.

Des alternatives libres existent et sont à soutenir.

7. Par où commencer ?

Si vous partez de zéro, la quantité de conseils dans ce guide peut paraître insurmontable. N'hésitez pas à améliorer progressivement vos pratiques. On propose donc divers ateliers qui peuvent être effectués séparément quand vous en sentez l'énergie ou le besoin. Pour les réaliser concrètement, de nombreux tutoriels se trouvent sur Internet. Le TuTORiel Tails[52] regroupe de nombreux tutoriels et constitue une bonne référence pour la plupart des ateliers proposés.

52 Brochure disponible sur Infokiosques.

1. Les attaques liées aux erreurs humaines

Les erreurs humaines sont la principale source d'attaques réussies.

1.1. Le shoulder surfing

On parle de shoulder surfing quand quelqu'un·e regarde ce qu'on écrit au-dessus de notre épaule. Cela peut être un mot de passe, le nom d'une adresse mail que l'on consulte ou un document sur lequel on travaille. On parlera aussi de shoulder surfing si une caméra arrive à voir notre écran et ce qu'on fait sur le support physique que l'on utilise.

Pour se protéger, on peut faire attention aux caméras, taper ses mots de passe de façon discrète sans avoir peur de passer pour paranoïaque ou tout simplement se mettre dans un coin de pièce quand on est sur notre ordinateur ou notre téléphone. On peut également acheter un filtre de confidentialité. Ce filtre empêche les personnes ne se trouvant pas en face de l'écran de le voir.

1.2. Les données sensibles qui traînent

De nombreuses attaques informatiques sont beaucoup plus simples à effectuer dès lors qu'on a un accès physique aux données en question. On pense par exemple aux téléphones qui finissent en garde à vue alors que cela aurait pu être prévisible (manifestation, action, etc.). Mais aussi à tout les vieilles clés USB, ordinateurs ou autres documents imprimés qui n'attendent qu'une perquisition pour finir dans les mains de l'État.

1.3. La mauvaise gestion des mots de passe

Les dangers : réutilisation des mêmes mots de passe, mots de passe courts, mots de passe non aléatoires

Plus un mot de passe est utilisé, plus sa sécurité baisse. En effet, quand vous donnez un mot de passe à une application ou un site Internet, vous ne pouvez pas être certain·es que cette application ou site stocke le mot de passe de manière sécurisée. Si les personnes à qui vous avez donné ce mot de passe se font attaquer, les attaquants peuvent récupérer votre identifiant et votre mot de passe et l'essayer sur d'autres services où vous avez donné un mot de passe. Les vols massifs d'identifiants sont

monnaie courante et il est probable qu'une de vos combinaisons identifiant et mot de passe ait déjà fuité sur Internet[1].

Une autre erreur concernant les mots de passe est leur robustesse trop faible. La robustesse d'un mot de passe dépend de nombreux paramètres comme sa longueur, l'utilisation de caractères spéciaux (majuscules, chiffres, etc.) et son caractère aléatoire.

De nombreuses études montrent que les humain·es sont prévisibles dans leurs choix de mot de passe. Des idées qui semblent malignes (mettre des nombres ou symboles au milieu de citations connues, etc.) sont en fait très standards et sont prises en compte dans les attaques par force brute.

Le conseil : mots de passe uniques, aléatoires & robustes

Pour toutes ces raisons, on conseille des mots de passe créés aléatoirement (et donc qui ne dépendent pas de choix humains), suffisamment robustes (c'est-à-dire qu'ils doivent être suffisamment longs) à usage unique (c'est-à-dire que chaque mot de passe n'est utilisé qu'une seule fois).

Cela peut paraître impossible à réaliser pour un·e humain·e de retenir des centaines de mots de passe complexes et aléatoires. C'est pour cela que plusieurs techniques ont été développées pour nous simplifier la vie. On va présenter une méthode recommandée par Tails[2]. Cette méthode est pensée dans le cas d'un modèle de menace assez sérieux (par exemple des agences gouvernementales pouvant consacrer un budget conséquent pour trouver un mot de passe) et donc est assez exigeante. Pour des usages moins sensibles, on peut se permettre d'alléger ces recommandations.

Première étape : créer quelques mots de passes mémorisables, robustes et aléatoires

On a vu que l'on ne pouvait pas se faire confiance à nous-mêmes pour choisir nos mots de passe car nous sommes trop prévisibles. C'est pourquoi on conseille la méthode Diceware pour fabriquer des phrases de passe mémorisables. Une phrase de passe est un mot de passe composé de mots aléatoires. Il est plus simple pour un humain de se souvenir de quelques mots plutôt que d'une suite de caractères et chiffres aléatoires.

1 Le site Have I been pwned recense des fuites de sécurité et vous dit si un mot de passe lié à votre adresse mail a pu fuiter lors d'une attaque informatique : https://haveibeenpwned.com/

2 Tails recommande l'article suivant de The intercept (en anglais) https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

6.5. Les téléphones : utilisation minimale et applications de messagerie via Internet

On peut essayer au maximum de garder nos téléphones loin de nous la plupart du temps. Cela nous forcera à moins compter sur eux et limitera notre dépendance à cet outil dangereux[51].

La dépendance aux outils téléphoniques comme Signal est un enjeu collectif de sécurité. Ainsi un groupe où il faut avoir Signal pour être intégré.e est un groupe qui met en danger toustes les personnes du collectif : par la dépendance à l'outil téléphonique et la centralisation des méthodes de communication.

Pour éviter d'être trop facilement espionnables, on peut utiliser des applications de messagerie par Internet comme Conversations pour le protocole XMPP ou Element pour Matrix tout en étant conscient·e que ces outils ne vous protègent pas contre tout les types d'attaques. Les applications de messagerie décentralisées qui ne demandent pas de numéros de téléphone pour fonctionner sont à préférer pour permettre aux personnes souhaitant limiter leurs dépendances à ces outils de participer (XMPP, Matrix).

On pourra aussi choisir d'utiliser au maximum des cartes SIM prépayées pour compliquer la géolocalisation de notre identité civile.

6.6. Ne pas laisser traîner ses appareils et les éteindre

Des attaques supplémentaires sont réalisables quand l'attaquant a :

- accès à un appareil numérique (téléphone, ordinateur) physiquement,
- accès à un appareil numérique allumé physiquement.

C'est pourquoi l'on recommande de faire attention à où on laisse ses appareils et à les éteindre quand on ne les utilise pas.

51 Le témoignage de Julie sur Cortana recueilli par la Quadrature du Net est édifiant sur les possibilités d'espionnage offertes par les téléphones portables.

Linux est l'autre choix naturel pour la protection numérique. Moins de virus existent sur Linux et en général les installateurs de Linux proposent le chiffrement du disque dur.

Il faudra par contre installer vous-mêmes Tor et vous y connaître pour protéger votre anonymat sur Internet notamment car de nombreuses applications communiquent sur Internet sans passer par Tor.

Windows ou Mac plutôt à éviter

Beaucoup de virus sont présents sur Windows alors que les Mac et Linux sont moins sujets aux virus. Ces derniers sont en effet des systèmes d'exploitation plus rares ce qui rend le développement de virus moins rentable. Cela est un point positif mais n'empêche absolument pas des développeurs malveillants de créer des virus pour Linux, Mac ou même Tails.

On conseille également d'éviter Windows et Mac tout simplement parce que les sociétés Microsoft et Apple sont des multinationales contre lesquelles de nombreux·ses militant·es luttent.

6.3. Faire des sauvegardes régulières de vos données

Les sauvegardes permettent de récupérer vos données en cas de perte de votre matériel informatique (accident, perquisition, etc.). Si vous utilisez Tails, il est possible de faire une copie conforme de votre clé Tails[50]. Pour les ordinateurs sur Linux, Windows ou Mac, vous pouvez avoir un disque dur chiffré où vous copiez les données que vous ne souhaitez pas perdre. Stockez vos sauvegardes dans des endroits à l'abri des perquisitions.

6.4. Sécuriser ses échanges mails

On pourra faire attention à créer plusieurs adresses mails selon les usages : personnel, militant, etc. On choisira également des serveurs d'hébergement de mail respectueux de la vie privée et variés.

On pourra également encourager à mettre en place le protocole PGP de chiffrement et encourager les personnes proches de nous à l'utiliser également.

50 Le site de Tails explique en détails comment créer une sauvegarde de sa clé Tails.

La méthode Diceware consiste à choisir des mots aléatoires parmi une liste de mots en lançant des dés à 6 faces (il existe des applications ou des logiciels de simulation de dés sur F-droid ou Linux). Des listes de mots Diceware ainsi que la méthode Diceware est expliquée sur Wikipédia[3].

Un mot de passe ayant plus de 5 mots aléatoires obtenus par Diceware est considéré comme robuste pour chiffrer une clé Tails à jour, une base de données de mot de passe ou un téléphone[4], etc[5] même face à des attaquants possédant des moyens considérables (agence gouvernementale par exemple). Quand on n'utilise pas Diceware pour créer la phrase de passe, le caractère moins aléatoire du choix des mots peut être compensé en rajoutant quelques mots à la phrase de passe.

Deuxième étape: utiliser un gestionnaire de mots de passe

Vous avez créé quelques phrases de passe robustes via la méthode Diceware. Ces mots de passe seront les seuls mots de passe dont vous vous souviendrez. Les autres seront créés et retrouvés via un gestionnaire de mots de passe. Les gestionnaires de mot de passe proposent de protéger une base de données contenant plusieurs mots de passe via un unique mot de passe qui permet de déverrouiller la base de données et d'accéder à tous les mots de passe qui sont dedans.

KeepassXC, le gestionnaire de mots de passe présent dans Tails

3 https://fr.wikipedia.org/wiki/Diceware

4 Les mots de passe de déchiffrement des téléphones sont gérés différemment selon les modèles et systèmes d'exploitation et il est donc dur de donner des recommandations claires. Il semblerait que pour les téléphones, on peut se permettre d'utiliser des phrases de passe ou des suites de chiffres moins longues (une douzaine de chiffres aléatoires suffirait dans la plupart des cas).

5 Dans les cas cités, on utilise des fonctions dites de dérivation de clés modernes comme argon2id pour Tails qui complexifient les attaques par force brute. Plus d'infos sur les fonctions de dérivation de clés sur un article de Tails et de Wikipédia https://tails.net/security/argon2id/index.fr.html et https://fr.wikipedia.org/wiki/%C3%89tirement_de_cl%C3%A9. Si aucune fonction de dérivation de clé n'était utilisée, il faudrait plutôt des phrases de passe avec 8 mots aléatoires.

Ces gestionnaires de mots de passe viennent avec des fonctions de génération de mots de passe aléatoires. Quand vous devez créer ou remplacer un mot de passe (parce que pas assez robuste), vous pouvez demander à votre gestionnaire de mot de passe de générer un mot de passe aléatoirement et de l'enregistrer. Quand vous aurez besoin du mot de passe, il n'y aura plus qu'à déverrouiller la base de données et à copier coller le mot de passe que vous aviez créé. Vu que vous n'avez pas besoin de mémoriser le mot de passe en question, cela ne coûte rien de choisir des mots de passe extrêmement robustes.

Pour la culture générale, nous mettons ci-dessous la table permettant de déterminer la robustesse d'un mot de passe selon sa longueur trouvée sur Wikipédia[6]. On insiste sur l'importance du terme aléatoire : une suite de chiffre ou de lettres ou de mots choisis par un humain ne peut être considérée aléatoire et possède donc une entropie beaucoup plus faible.

Nombre de symboles / Entropie du mot de passe (ou robustesse)	Chiffres arabes (0-9) aléatoires	Chiffres arabes et Lettres (0-9 et aAbB...) aléatoires	Chiffres arabes et lettres et symboles (0-9 et !&? et aAbB...) aléatoires	Mots tirés aléatoirement parmi une liste de mots comprenant 7776 mots (nombre de combinaisons de 5 dés à 6 faces)
32 bits (environ 10^{10} combinaisons possibles)	10	6	5	3 mots
64 bits (environ 10^{19} combinaisons possibles)	20	11	10	5 mots
80 bits (environ 10^{24} combinaisons possibles)	25	14	13	7 mots
96 bits (environ 10^{28} combinaisons possibles)	29	17	15	8 mots
128 bits (environ 10^{38} combinaisons possibles)	39	22	20	10 mots
160 bits (environ 10^{48} combinaisons possibles)	49	27	25	13 mots

L'entropie du mot de passe permet de déterminer la difficulté à deviner le mot de passe : plus l'entropie est haute, plus le mot de passe est robuste. Selon la technique d'étirement de clés utilisés, les recommandations d'entropie pour qu'un mot de passe soit considéré comme robuste sont différentes. Pour les méthodes modernes, on considère qu'il suffit de 64 bits avec les capacités de calcul actuelles. S'il n'y a pas de techniques d'étirement de clés, il vaut mieux compter 96 bits. L'estimation du temps de calcul (et du prix) nécessaire pour deviner un mot de passe dépend fortement de la technique d'étirement de clés et du caractère réellement aléatoire du mot de passe.

6 https://fr.wikipedia.org/wiki/Robustesse_d%27un_mot_de_passe

6.2. Bien choisir son système d'exploitation pour son ordinateur

On pourra différencier les systèmes d'exploitation selon les usages que l'on fait (personnel, militant, travail, etc.). On pourrait ainsi avoir une clé Tails pour un usage militant et un ordinateur avec Linux pour un usage plus personnel (famille, achats en ligne, etc.).

Le système d'exploitation Tails est facilement utilisable par une personne ayant peu de connaissances informatiques[48]. Parmi les avantages qu'une clé Tails offre, on peut citer entre autres :

- Tails propose un environnement qui vous protège contre un grand nombre d'attaques et vous empêche de faire certaines erreurs,
- Tails vient équipé en applications pratiques,
- Tails passe par Tor systématiquement pour l'intégralité des connexions à Internet,
- les utilisateur·ices de Tails se ressemblent sur Internet ce qui procure une certaine forme d'anonymat,
- les données dans le stockage persistent d'une clé Tails sont chiffrées via LUKS.

Les problèmes de Tails sont les suivants :

- complexité d'installer d'autres applications que celles fournies de base,
- le fait de passer par Tor systématiquement empêche parfois de se connecter à des services que vous utilisiez d'habitude,
- surveillance considérable de Tails et attaques quelques fois réussies contre Tails[49],
- Tails peut donner un faux sentiment de sécurité ce qui est dangereux.

Linux, plus compliqué à protéger mais plus flexible

48 Un tutoriel pour apprendre à utiliser Tails est disponible sur Infokiosques.net
49 Tails recense de nombreuses limitations à Tails sur leur site.

Pour faire confiance aux clés de chiffrement, on peut vérifier les empreintes des clés que l'on utilise. Cela permet de se protéger de l'attaque de l'homme du milieu[44]. On peut le faire sur Signal et Conversations en cherchant dans les paramètres. Pour le protocole PGP, les clés ont également une empreinte que l'on peut vérifier visuellement ou via un autre moyen de communication[45]. ou vérifier par d'autres moyens (en vérifiant l'empreinte visuellement par exemple) que l'on a les bonnes clés publiques.

6. En pratique, que faire ?

Tout dépend du modèle de menaces envisagé. Ces différents conseils ne sont donc pas adaptés à toutes les situations même si on a essayé de les penser assez généralistes.

6.1. Prendre au sérieux la surveillance numérique

Ce guide n'est pas uniquement pour les militant·es aguerri·es. La surveillance numérique fonctionne grâce à l'espionnage d'un grand nombre de personnes[46] y compris des personnes qui pensent n'avoir rien à cacher[47]. Les données récupérées en masse sont ensuite analysées par ordinateures.

Dans une conversation à plusieurs, c'est la personne la moins protégée qui détermine le niveau de sécurité de la conversation. Se protéger, c'est donc aussi protéger les autres, par exemple en leur proposant de l'aide pour améliorer leurs pratiques si iels souhaitent le faire. **La surveillance est un enjeu collectif et non individuel.**

44 https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

45 Il existe également des serveurs de clés hébergeant des clés publiques et sur lesquels des individus peuvent signaler avoir vérifié que telles adresses correspondent bien aux personnes qu'elles revendiquent être. Cela permet de fonctionner via un système de toile de confiance (je fais confiance à A qui fait confiance à B qui fait confiance à C donc je fais confiance à C). Plus d'infos sur le sujet sur wikipédia : https://fr.wikipedia.org/wiki/Toile_de_confiance

46 La quadrature du net dénonçait en 2020 les décrets pasp qui permettent le fichage massif des militants politiques. https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/

47 Pour vous convaincre que tout le monde a quelque chose à cacher, https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

1.4. Les réseaux sociaux

La quantité d'informations que l'on peut donner sur nous-mêmes sur un réseau social est considérable. Utiliser un compte sur un réseau social pour consulter des informations militantes, c'est offrir à la police et aux géants du Web (Facebook, Twitter, Instagram, etc.) des données que l'on souhaiterait probablement garder cachées[7]. En utilisant les réseaux, on renforce des géants du capitalisme en leur fournissant un pouvoir considérable sur nous et nos luttes[8].

Il peut paraître compliqué de quitter d'un jour à l'autre un réseau social que l'on utilise très régulièrement pour communiquer et s'informer. C'est pourtant ce que l'on conseille. Pour faciliter la transition, vous pouvez essayer de déterminer pourquoi vous avez l'impression d'avoir besoin des réseaux sociaux. Les réseaux sociaux sont conçus pour se rendre indispensables et addictifs et créent un sentiment de dépendance et on trouve intéressant de questionner cette dépendance.

Si vous utilisez les réseaux sociaux pour vous informer, on vous conseille d'utiliser les flux RSS[9]. Si c'est pour rester en contact avec d'autres collectifs, vous pouvez leur demander d'utiliser d'autres moyens de communications (listes mails, publier sur les réseaux Mutu ou sur un site Internet leurs contenus, etc).

Si vous utilisez les réseaux sociaux pour toucher un grand nombre de personnes dans une optique militante, on vous conseille de faire attention à poster systématiquement vos contenus sur d'autres supports. Sinon votre capacité à informer les autres dépendra d'une plateforme centralisée qui peut être censurée et vous excluerez les militant·es qui font le choix de ne plus utiliser les réseaux sociaux[10].

Si vous aimez quand même le concept des réseaux sociaux par exemple pour rester en contact avec des ami·es, le réseau Mastodon[11] est plus respectueux de la vie privée même s'il est loin d'être exempt de certains défauts (l'addiction par exemple). Vous pouvez aussi choisir de ne plus poster sur les réseaux sociaux tout en gardant votre compte et en le consultant épisodiquement, vous garderez ainsi contacts avec vos ami·es. Cependant notez bien que les réseaux sociaux sont conçus pour vous attirer donc cette stratégie est complexe à mettre en place dans la pratique.

7 Le documentaire Nothing to hide montre à quel point on peut se tromper sur le degré de détail que les réseaux sociaux et autres entreprises qui récupèrent nos métadonnées peuvent avoir sur nous.

8 La brochure Face à Facebook disponible sur infokiosques permet de se rendre compte de ce que peut faire Facebook avec le pouvoir qu'on lui donne en l'utilisant.

9 Le site Infokiosques.net propose quelques tutoriels pour apprendre à utiliser les flux RSS

10 https://zadducarnet.org/index.php/2020/10/30/lettre-a-celleux-qui-militent-sur-les-reseaux-sociaux/

11 https://joinmastodon.org/

1.5. Les métadonnées des fichiers

Les photos, fichiers PDF ou textes peuvent contenir des métadonnées qui renseignent sur l'heure de dernière modification, la marque de l'appareil photo (pour les photos) et pleins d'autres informations. On conseille de les supprimer systématiquement dès que l'on partage un fichier. Le système d'exploitation Tails intègre le logiciel Nettoyeur de métadonnées pour supprimer les métadonnées. Ce logiciel est téléchargeable pour Linux et sinon des sites web proposent de supprimer les métadonnées pour vous via mat2[12].

1.6. Le social engineering

On parle de social engineering quand des personnes nous soutirent des informations que l'on souhaiterait idéalement garder secrètes via des manipulations psychologiques. Cela peut se faire par exemple lors d'une discussion par une question anodine.

La méthode de protection face au social engineering est tout autant collective qu'individuelle. Ne pas être curieux.ses ou poser des questions indiscrètes, cela se travaille[13]. Pour aider les gens à oser dire non aux questions auxquelles iels ne souhaitent pas répondre, on peut faire en sorte que cela soit tout à fait accepté dans un collectif sans qu'il y ait de conséquences négatives sur l'image que l'on donne.

2. Attaques spécifiques aux téléphones portables

On essayera de voir les spécificités et quelques mesures de protections face aux attaques suivantes :

- récupération des données que stockent les fournisseurs d'accès téléphoniques,
- récupération des données que stockent les applications de vos téléphones (par exemple via une perquisition d'un téléphone lors d'une garde à vue),
- prise de contrôle d'un téléphone à distance (via divers bugs d'applications).

Toutes ces données peuvent être récupérées légalement ou illégalement par la police. Les données récupérées illégalement ne peuvent pas être utilisées lors des instructions

12 https://metadata.systemli.org/ . Notez que la suppression des métadonnées d'un PDF le rend souvent plus lourd et empêche le copier-coller. En ligne de commande, on peut utiliser l'option `mat2 --lightweight fichier.pdf` pour éviter ces effets indésirables.

13 Pour plus d'informations sur le sujet, on pourra lire Culture de la sécurité de Crimethinc sur Infokiosques

Dans le cas d'une application décentralisée, les métadonnées des conversations sont stockées sur des serveurs différents. Si les autorités arrivent à accéder à un des serveurs hébergeant l'application de messagerie, elles auront accès seulement aux métadonnées qui ont transitées via ce serveur et pas aux métadonnées d'autres conversations passant par d'autres serveurs. Les applications décentralisées sont également moins sensibles aux attaques par déni de service[41] pour bloquer les communications.

Une attaque spécifique aux applications utilisant un numéro de téléphone comme Signal, Telegram ou WhatsApp est la suivante. Les autorités pourraient demander à un opérateur une copie de votre carte SIM, installer Signal dessus et récupérer ainsi l'intégralité de vos messages sur un smartphone qu'ils possèdent[42] si elles ont accès au code PIN que vous avez donné à Signal.

Pour vous protéger de cette attaque, pensez à choisir un code PIN long et unique à votre compte Signal. Choisissez de même un mot de passe sécurisé pour vos comptes XMPP ou Matrix.

Remarquez aussi que vos conversations passées peuvent laisser de nombreuses traces sur vos téléphones ou ordinateurs et que cela peut être embêtant en cas de perquisition ou saisie de votre matériel (garde à vue, etc.). On conseille donc de faire en sorte que les messages ne soient pas stockés de manière permanente sur vos appareils par exemple en activant l'option de messages éphémères disponibles sur certaines applications.

5.4. Fiabilité des mécanismes de chiffrement

L'attaque frontale des mécanismes de chiffrement demande une puissance de calcul considérable. La seule menace concrète pour des particuliers est en cas d'évolution de technologie permettant de calculer beaucoup plus rapidement qu'avant ce qui compromettrait l'ensemble messages chiffrés du passé. Certains mécanismes ont intégré ce risque pour éviter qu'on puisse déchiffrer un vieux message après un certain temps[43].

41 La messagerie Telegram a été attaquée à Hong Kong en 2019 pendant des manifestations massives ce qui a bloqué l'organisation des manifestant.es https://theconversation.com/how-a-cyber-attack-hampered-hong-kong-protesters-118770

42 https://dijoncter.info/qu-est-ce-qu-on-connait-de-signal-1510. Pour une critique plus détaillée de Signal, on pourra consulter une brochure traduite en français de l'américain : https://iaata.info/Parlons-de-Signal-3517.html.

43 On pourra voir la notion de confidentialité persistante sur wikipedia.

5.3. Signal, WhatsApp, Telegram, XMPP, Matrix

Signal, WhatsApp, Telegram, XMPP, Matrix utilisent des protocoles de chiffrement bout-à-bout avec quelques spécificités selon les protocoles sur lesquels on ne s'attardera pas ici[38]. Ce principe assure que les seuls appareils ayant les clés de déchiffrement des messages sont ceux des correspondant·es. Les serveurs qui permettent la conversation (par exemple celui de Signal) ne peuvent pas déchiffrer les conversations. Ainsi si les autorités piratent uniquement les serveurs de Signal, ils n'auront pas accès aux messages mais seulement aux métadonnées.

Ce chiffrement bout-à-bout ne protège par contre pas d'attaques visant les appareils des correspondant·es et les autorités essaient de trouver des solutions pour avoir accès aux messages via des failles[39].

Signal, Telegram et WhatsApp utilisent votre numéro de téléphone portable. Cela est un risque car comme on l'a vu, les autorités peuvent récupérer votre nom via un numéro de téléphone portable si vous payez un abonnement à votre nom.

C'est pourquoi l'on préfère XMPP ou Matrix qui demandent juste un compte XMPP ou un compte Matrix pour fonctionner ce qui est plus anonymisable. À défaut, on préfèrera Signal à Telegram ou WhatsApp car Facebook possède WhatsApp et Telegram envisage de se financer via de la publicité.

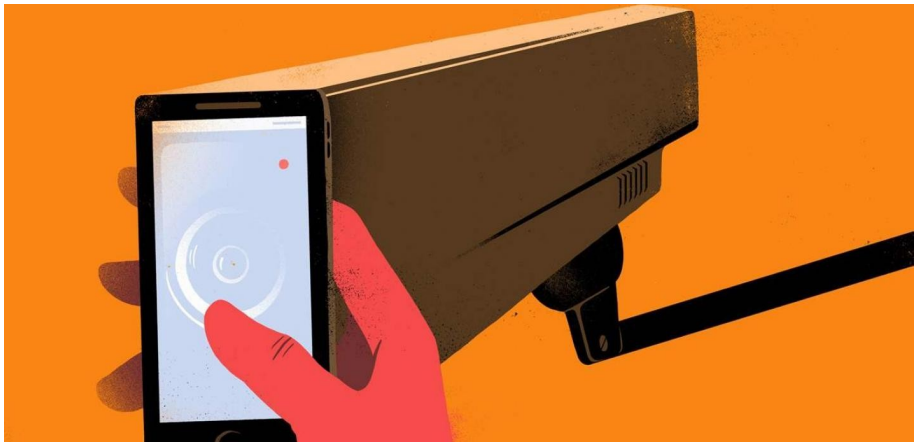
On pourra aussi essayer d'enregistrer un compte avec un faux numéro de téléphone ; diverses techniques sont possibles.

XMPP et Matrix sont des applications décentralisées ce qui peut compliquer la tâche des autorités pour récupérer des métadonnées. En effet les applications centralisées centralisent ces métadonnées sur un seul serveur. Si les autorités arrivent à accéder au serveur de Signal (par piratage ou coopération de Signal), ils auront accès aux métadonnées de toutes les conversations passant par Signal. Les applications centralisées sont beaucoup plus facilement censurables ou sujet à chantage : il suffit de fermer leurs serveurs pour les bloquer[40] (ou de les menacer de fermer leurs services pour les forcer à obéir).

XMPP est un protocole de messagerie instantanée libre et décentralisé. Plus d'infos pour comment utiliser XMPP sur joinjabber.org

38 https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_protocols
39 Voir l'article du 24/05/2017 sur https://attaque.noblogs.org/files/2020/06/french_intelligence_fr.pdf
40 Récemment, Tiktok a été bloqué pendant la révolte kanak en 2024.

judiciaires mais peuvent l'être pour mettre la pression afin de récolter des aveux, de faire parler. Il est donc important de ne rien déclarer et ne rien avouer en garde à vue quoi que l'on nous montre ou dise[14]. Au stade de la garde à vue, on ne peut pas vérifier ce que la police a sur nous de manière légale, il vaut donc mieux attendre de voir un.e avocat.e ou des ami.es avant de déterminer une stratégie de défense.



La présentation faite ici est assez courte. Pour avoir plus de détails sur les enjeux de sécurité numérique liés aux téléphones, on peut consulter la brochure Téléphonie mobile (2023) disponible sur infokiosques.net.

2.1. Les données accessibles via les opérateurs téléphoniques : géolocalisation et métadonnées

Tout ce que l'on dit dans ce paragraphe concerne tous les téléphones portables, qu'ils soient dits intelligents ou pas.

Dès qu'un téléphone est allumé sans mode avion, il communique très régulièrement avec les antennes proches (qu'il ait une carte SIM ou non). Le téléphone communique le numéro de la carte SIM active dans le téléphone ainsi que le numéro IMEI de l'emplacement de la carte SIM. Le numéro IMEI est un numéro de série qui identifie de manière unique le téléphone. Ce signal envoyé aux antennes permet de géolocaliser le téléphone via une triangulation (en connaissant approximativement la distance des 3 antennes les plus proches, on retrouve la position du téléphone).

14 Pour se renseigner à ce sujet, on conseille la BD disponible sur infokiosques.net : En GAV, je n'ai rien à déclarer.

Dès que vous passez un appel ou envoyez un SMS, les opérateurs téléphoniques stockent les métadonnées de ce coup de fil ou SMS pendant 2 ans dans la facture détaillée. Ces métadonnées consistent en : géolocalisation approximative des deux correspondant.es, date et heure de la communication ainsi que durée de l'appel.

Attaque possible : récupération des métadonnées et de la géolocalisation via une simple demande

La police peut demander aux opérateurs les informations suivantes de manière automatique et très rapide[15] (le prix fixé au journal officiel en 2012 est entre parenthèses) :
- identification d'une personne via son numéro de téléphone (4,59 euros),
- obtenir la facture détaillée d'un numéro de téléphone (15,30 euros),
- mettre sur écoute un numéro de portable (24 euros),
- liste des numéros utilisant telle borne de télécommunication (12,75 euros),
- en cas de cartes prépayées, la police peut demander où a été vendue cette carte pour 15,30 euros,
- les adresses IP (sites internet, serveurs, etc.) auxquelles un téléphone se connecte.

Comment marche schématiquement la surveillance automatisée de masse des militant.es

La facture détaillée d'un numéro de téléphone contient de nombreuses informations analysables facilement de manière automatique. C'est un moyen d'enquête utilisé massivement. Un exemple d'utilisation de ces données est le suivant : on attribue à chaque personne un score de dangerosité via ses déplacements dans des lieux de lutte et ses communications avec d'autres militant·es. On peut ainsi détecter de nouveaux lieux de luttes de manière totalement automatisée en remarquant que beaucoup de personnes avec un haut score de dangerosité s'y rendent. De même on peut détecter les nouveaux et nouvelles militant·es via les communications qu'iels ont avec d'ancien·nes militant·es et leur passage dans des lieux de lutte. Cet exemple est particulièrement important pour comprendre que la surveillance de masse est un **enjeu collectif et non un enjeu individuel.**

Face à la géolocalisation : cartes SIM prépayées et ne pas toujours prendre son téléphone avec soi

Il est possible d'utiliser des cartes SIM prépayées (Lebara, Lycamobile par exemple). On peut associer à ces cartes prépayées une autre identité (imaginaire, etc.) que son identité civile. Il n'empêche que la carte SIM prépayée sera quand même géolocalisée régulièrement. De plus, les autorités pourraient recouper l'identité choisie pour une carte SIM prépayée avec une identité civile un jour.

15 https://blogs.mediapart.fr/louise-fessard/blog/260312/ecoutes-ce-que-la-police-peut-obtenir-des-operateurs

maintenus par des militant.es états-unien.nes et peuvent être victimes d'attaques ciblées car de nombreux.ses militant.es politiques les utilisent. De l'autre côté, Google automatise la lecture des mails en transit sur leurs serveurs pour y récupérer des données et les analyser.

Pour se protéger face aux attaques sur les serveurs mails que vous utilisez, vous pouvez :

- utiliser le protocole PGP de chiffrement des mails pour que même le serveur mail n'ait jamais accès à vos mails sans votre clé privée personnelle,
- essayer de décentraliser vos données au maximum et ne pas tout mettre sur les mêmes serveurs (on devrait ainsi éviter de toustes utiliser Riseup)[35].

Un des dangers de la centralisation des adresses mails sur les mêmes serveurs (par exemple riseup[36]) est l'attaque par déni de service (DoS). Un attaquant peut empêcher toustes les utilisateur·ices d'un même serveur d'accéder à leurs mails pendant un laps de temps en attaquant ce serveur. Cette attaque peut bloquer vos communications. Elle est similaire dans ce sens au brouillage d'antennes réseau pour la téléphonie mobile.

Une adresse mail peut tendre vers l'anonymat si vous compartimentez ses usages. Avoir plusieurs adresses mails différentes est bénéfique pour séparer vie personnelle, travail et activité militante. Sinon les autorités peuvent retrouver plus aisément votre identité via votre adresse mail. On pourra aussi choisir d'avoir plusieurs adresses mails[37] selon les lieux de lutte que l'on visite de la même manière qu'on pourra choisir différents pseudos selon les lieux de lutte sur lesquels on va.

Si le disque dur est chiffré, les clients mails sont bien pratiques notamment si on a plusieurs adresses mails car on compartimente les adresses selon les usages. On peut les configurer pour que la connexion aux serveurs mails passent par Tor ; cela est fait automatiquement sur Tails. Si l'on utilise le protocole PGP, il est plus simple d'utiliser des clients mails comme Thunderbird que de consulter ses mails sur le Webmail.

35 CHATONS propose des services libres et décentralisés comme par exemple l'hébergement d'adresse mails. On pourra cependant préférer pour des raisons judiciaires des services à l'étranger. Riseup recense aussi une liste de serveurs engagés. On déconseille protonmail pour plusieurs raisons : entreprise capitaliste, incompatibilité de la version gratuite avec l'utilisation d'un client mail et collaboration avec la justice...

36 Le blocage des invitations par riseup en 2023 peut être ainsi interprété comme une bonne nouvelle pour forcer la décentralisation. Notez que d'autres serveurs radicaux proposent des adresses mails (autistici.org, immerda.ch, etc.)

37 Si vous avez une adresse mail riseup, vous pouvez créer des alias https://riseup.net/aliases

Il est également facile d'usurper des identités via mail. Il peut être difficile d'être certain.es que la personne à laquelle on écrit est bien la personne que l'on imagine.

Un système de chiffrement dit bout-à-bout est un système qui chiffre les communications de manière à ce que seul·es le ou la destinataire et l'expéditeur·ice puisse déchiffrer. Le système TLS n'est donc pas un système de chiffrement bout-à-bout.

Pour nous protéger à la fois des usurpations d'identité et du non chiffrement de nos mails, on recommande d'utiliser le protocole PGP[34] qui est un mécanisme de chiffrement bout-à-bout que vous contrôlez. Vous n'aurez plus à faire confiance à d'autres acteurs pour bien chiffrer vos données vu que vous le ferez vous-mêmes. Vous pouvez également vérifier en comparant les empreintes des clés si la personne pour laquelle vous chiffrez correspond bien à la personne que vous pensez.

Les métadonnées de vos communications mails (heure d'envoi, émetteur et destinataire) restent accessibles à de nombreux acteurs quels que soient le protocole.

Logiciel de messagerie ou webmail ?

Les logiciels de messagerie comme Thunderbird, Outloook ou l'application « Mails » d'Apple permettent de centraliser sur une même application plusieurs adresses mails. On conseille de les utiliser uniquement si le disque dur de l'ordinateur est chiffré car sinon toute personne ayant accès à votre ordinateur pourra lire vos mails. Il faudra préférer consulter systématiquement ses adresses mails sur un navigateur si le disque dur n'est pas chiffré afin de ne pas stocker le contenu des mails en clair. Si l'on souhaite compliquer l'identification entre une adresse mail et une identité civile, il faudra consulter ses mails systématiquement via Tor (une seule erreur suffit à créer une association!)

5.2. Hébergeur d'adresse mails

Selon l'adresse mail que vous avez, vos données sont stockées sur des serveurs différents (les serveurs de riseup pour les adresses riseup, les serveurs de Google pour Gmail, etc.). Ces serveurs ont souvent accès au contenu de vos mails si vous n'utilisez pas le protocole PGP. Ils ont en tout cas accès aux métadonnées des mails, c'est-à-dire aux heures des communications et aux adresses mails qui communiquent.

Choisir un hébergeur mail, c'est choisir à quel serveur vous faites confiance. Faites vous plutôt confiance à Riseup ou à Google ? D'un côté, les serveurs de Riseup sont

34 La Frree Software Foundationne donne sur leur site plusd'infos sur comment mettre en place le protocole PGP https://emailselfdefense.fsf.org/fr/

Notez bien que si vous mettez une nouvelle carte SIM prépayée dans un téléphone que vous utilisiez auparavant, le numéro IMEI du téléphone reste le même. Cela permet d'établir un lien entre vos deux identités. Si vous achetez un téléphone neuf avec un moyen de paiement nominatif, le numéro IMEI du téléphone sera aussi relié à votre identité. Pour compliquer la tâche des autorités de relier l'identité liée à la carte SIM prépayée avec votre identité civile, utilisez un téléphone acheté cash où vous n'avez jamais mis de cartes SIM à votre nom.

Des solutions partielles comme les cartes SIM prépayées sous des faux noms peuvent considérablement compliquer le travail de la justice. Même si les services de renseignement arrivent à relier votre identité imaginaire à votre identité civile d'une façon ou d'une autre, ils devront encore le prouver aux juges.

Pour éviter d'être géolocalisé·e, on peut choisir de ne pas prendre systématiquement son téléphone avec soi et ne le consulter qu'à un lieu quasi-fixe. Faites attention, les changements d'habitude abrupts (éteindre son téléphone juste avant une manifestation par exemple) sont facilement repérables par une analyse automatisée. Il vaut mieux essayer de varier ses habitudes de connexion régulièrement (éteindre son téléphone en dehors de cadres militants par exemple).

Pour plus d'informations sur la surveillance de masse liée aux villes intelligentes, lire le manifeste sur le site technopolice.fr.

Pour laisser moins de métadonnées, utiliser les applications de communication via Internet

Pour protéger nos données de ces attaques de la police, on peut choisir de communiquer via nos téléphones exclusivement en utilisant nos connexions Internet via diverses applications comme Signal, Conversations ou Element (voir plus tard la partie sur les systèmes de messagerie instantanées). Ainsi les opérateurs téléphoniques (et donc la police via les demandes aux opérateurs) auront accès à moins de métadonnées. En effet, l'opérateur téléphonique saura juste que vous demandez à communiquer avec le serveur de Signal à telle heure et pas avec qui vous souhaitez communiquer.

Face aux écoutes, choisissez bien vos sujets de discussion par téléphone

N'hésitez pas à couper votre interlocuteur·ice si iel parle d'un sujet sensible par téléphone. Cela n'est absolument pas le bon moyen de communication pour ce genre de discussions car les SMS et appels ne sont pas chiffrés et donc visibles par l'opérateur ainsi que par la police en cas de mise sur écoute.

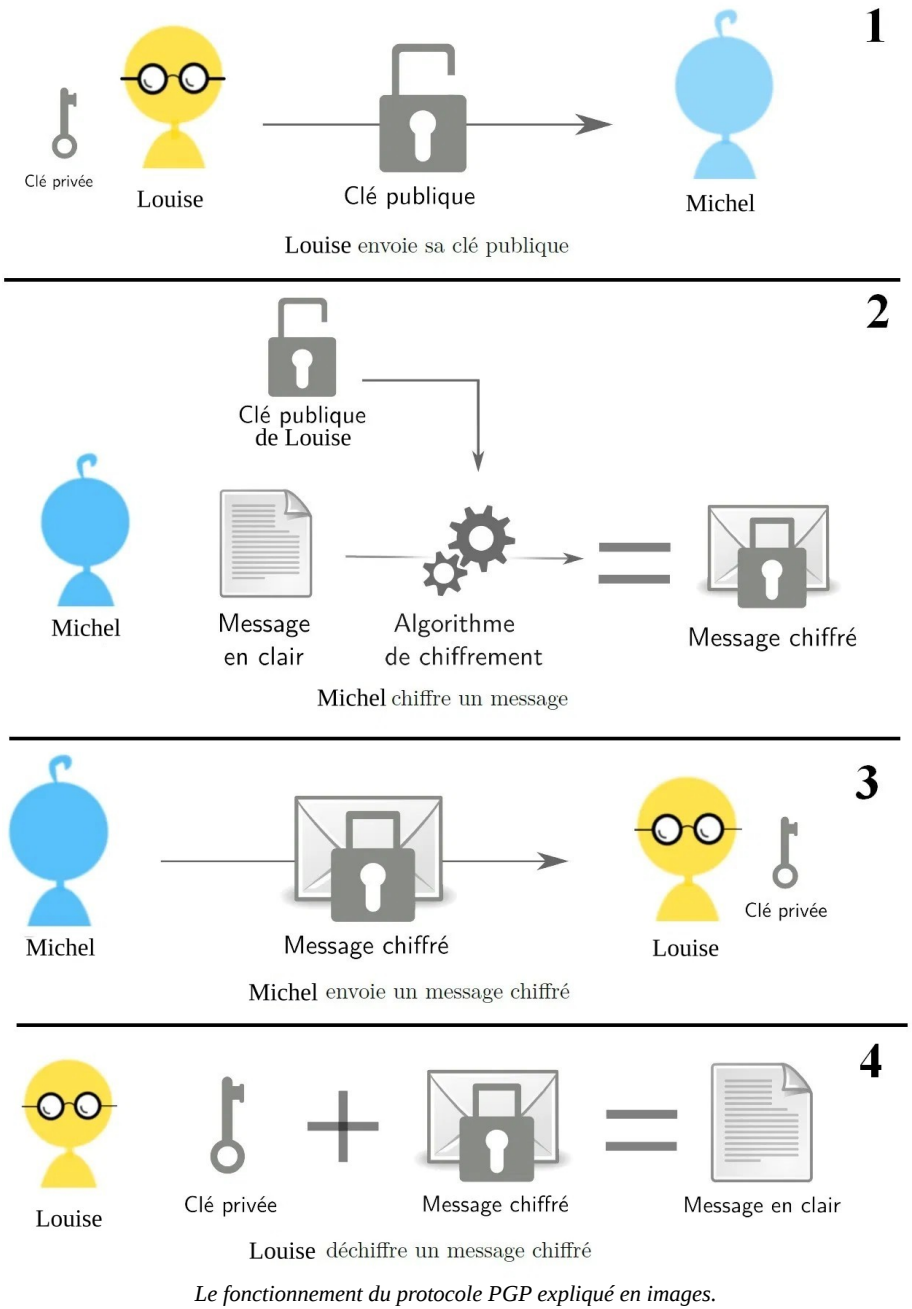
Il est important de noter que les écoutes sont enregistrées numériquement, stockées et peuvent resservir des années plus tard lors d'une enquête.

2.2. Données accessibles via les applications de vos téléphones

Quasiment toutes les applications installées stockent des données à la fois sur votre téléphone et sur des serveurs distants (le « cloud »). La police peut récupérer ces données par exemple en ayant accès à votre téléphone pendant une garde à vue ou en accédant à votre téléphone via une perquisition ou en demandant aux hébergeurs de l'application les données qu'ils ont sur vous.

Ces données peuvent être les suivantes :

- pour les applications de messagerie, l'intégralité de vos messages potentiellement même ceux supprimés,
- pour les applications de type GPS, toutes les adresses que vous avez rentrées dans l'application ainsi que l'historique des trajets effectués avec,
- pour les applications d'achats, l'historique de vos achats, vos cartes bleues enregistrées, vos recherches,
- pour les navigateurs Web, votre historique de navigation (même s'il est supprimé de votre téléphone si les serveurs de l'application le stockent),
- vos photos, vidéos, etc,
- vos contacts.



Le fonctionnement du protocole PGP expliqué en images.

L’empreinte d’un navigateur Firefox est par contre souvent moins anonyme que l’empreinte d’un Tor Browser. On recommande de ne pas utiliser des navigateurs qui empêchent les extensions protectrices de la vie privée de fonctionner convenablement car la revente de données personnelles est le coeur de leur modèle économique (chrome, edge, etc.).

5. Attaques spécifiques aux systèmes de messagerie instantanées

Ce qu’on dit ici s’applique à tout type de conversations, qu’elles soient à deux ou à cent. Cependant, notez que la principale attaque contre les services de messagerie instantanée est l’infiltration sur les grands groupes de conversations. Cela n’est souvent pas compliqué pour la police à mettre en place – il suffit de faire en sorte qu’une personne soit ajoutée à la conversation – et donne accès à beaucoup d’informations. Méfiez vous donc des conversations à beaucoup et n’y donnez pas d’informations sensibles.

Les conversations qui passent via Internet sont souvent chiffrées : Signal, XMPP, Matrix, mails, etc. On va essayer de comprendre comment ça se passe précisément pour mieux visualiser les risques de ces mécanismes de chiffrements.

Quand un message va de Louise à Michel via Internet, des données transitent via de nombreux intermédiaires. Les systèmes de chiffrement font en sorte que ces serveurs intermédiaires ne puissent pas déchiffrer ces données en le contenu du message entre Louise et Michel.

Si aucun mécanisme de chiffrement n’est mis en place pour une conversation sur Internet, cela signifie que des attaques sur n’importe quel serveur intermédiaire permettent de récupérer la conversation.

5.1. Transfert des mails

La plupart des clients mails utilisent le protocole TLS qui est un système de chiffrement. Ce protocole chiffre la communication entre les serveurs mails de l’expéditeur·ice et du destinataire[33].

Cependant les serveurs de mails ont accès aux communications et peuvent les lire. Par exemple, si vous utilisez un compte Gmail, Google lit vos communications et récupère les données.

33 Il s’agit du même protocole qui est utilisé lors de la consultation de page web via HTTPS.

Mesures de protection : chiffrer votre téléphone et limiter les données des applications

Vous ne pouvez pas garantir que les autorités n’auront pas accès aux données que vos applications stockent. Lors d’une perquisition d’un téléphone, considérez que toutes les données de votre téléphone sont accessibles aux autorités si elles souhaitent en mettre les moyens. Vous pouvez essayer de ralentir la police au maximum en choisissant de chiffrer votre téléphone avec un code de déverouillage long. Cette option est disponible sur de nombreux systèmes d’exploitation. Cependant sachez que le chiffrement des données ne sera utile que si le téléphone est saisi quand il est éteint. On ne connaît pas les moyens précis de déchiffrement des smartphones que les flics ont a disposition et cela dépend des marques de téléphones et des systèmes d’exploitation.

La stratégie de protection principale est donc tout simplement de limiter les données que stockent les applications de votre téléphone. Sur toutes les applications, vous pouvez modifier les paramètres de confidentialité. Mettez les au maximum systématiquement.

Des mouchards peuvent avoir été mis facilement dans tout appareil électronique qui a passé un moment dans les mains de la police loin de votre surveillance

Mesure de protection : ne pas se fier aux applications financées en revendant vos données

Dans la mesure du possible, désactivez le stockage de vos données sur le cloud ce que de nombreux téléphones et nombreuses applications font automatiquement. Vos données ne devraient être stockées que en local sur votre téléphone et non sur des serveurs distants. Cela peut être compliqué à faire avec certaines applications comme celles que les GAFAM[16] proposent.

Vous ne pourrez en effet jamais faire confiance à des applications qui se financent en revendant vos données pour ne pas conserver vos historiques de données. Choisir des logiciels dits libres[17], c’est quelques fois trouver des applications faites par des personnes luttant pour la vie privée sur Internet et contre la surveillance de masse.

16 GAFAM désigne des géants du Web (Google, Apple, Facebook, Amazon, Microsoft). Pour savoir ce que beaucoup de militant·es reprochent aux GAFAM, on pourra se renseigner sur un site de la quadrature du net https://gafam.laquadrature.net/

17 Pour plus d’information sur le mouvement du logiciel libre, on peut consulter la page Wikipedia Logiciel libre et la carte des alternatives de Framasoft.

Ainsi pour installer des logiciels sur Android, on recommande d'utiliser F-Droid et non le Google Play Store. De même on préférera Organic maps comme application GPS, Firefox ou Tor Browser comme navigateur Web.

En général, essayez de limiter au maximum votre dépendance aux GAFAM. On recommande ainsi de limiter au maximum la présence sur les réseaux sociaux (Twitter, Facebook, Instagram, etc.), de ne pas utiliser Chrome ou Gmail, etc.

Notons également qu'il existe des systèmes d'exploitation libres (donc qui remplacent Android par exemple) pour les téléphones mais qu'ils peuvent être compliqués à installer[18].

Des listes plus complètes d'applications et de systèmes d'exploitation libres se trouvent par exemple dans la brochure Téléphonie mobile sur infokiosques.net publiée en 2023 (notez que ces listes ne sont pas faciles à mettre à jour).

2.3. Prise de contrôle à distance d'un téléphone

On quitte ici le domaine de la surveillance de masse pour la surveillance individuelle. Cette différence est cruciale car la grande majorité de la surveillance est automatisée. En comparaison, la surveillance individualisée qui demande plus de moyens humains est beaucoup plus chère à mettre en place et donc plus rare.

Les services de renseignement ont eu les moyens de prendre le contrôle total des téléphones à distance et l'ont probablement encore aujourd'hui. On ne sait pas exactement si cela est facile ou pas, si cela est fréquent ou pas et cela dépend des marques des téléphones mais cela est une possibilité.

Cette attaque permet entres autres de :

- noter tout ce qui est écrit dans le téléphone (mots de passes, etc.)

- activer le micro à distance,

- activer la caméra à distance.

Face à cette attaque, il y a peu à faire. On peut essayer de l'empêcher en amont en installant le moins d'applications possibles et en désactivant le Bluetooth. C'est souvent via des failles de sécurité du Bluetooth ou d'une application que l'attaquant

18 Certains systèmes d'exploitation libres existent pour des téléphones. Au moment de l'écriture de ce guide (2024), les deux systèmes d'exploitations les plus appréciés sont GrapheneOS et DivestOS mais attention ces systèmes ne sont compatibles qu'avec certains téléphones (seulement les Pixel pour GrapheneOS). Plus d'infos sur GrapheneOS (en anglais) sur anarsec.guide : https://www.anarsec.guide/posts/grapheneos/

- le fait que vous avez choisi de rester authentifié plusieurs jours d'affilée,
- l'historique des marchandises que vous avez regardé sur un site d'achat en ligne,
- les vidéos que vous avez regardées,
- etc.

Le navigateur Tor browser répond de manière efficace à ces 3 attaques (espionnage des communications http, analyse de l'empreinte du navigateur et cookies malveillants qui nous traquent) :

- la navigation web passe obligatoirement par Tor browser sur lequel est installé le mode https only qui force les sites internet à utiliser https (et prévient l'utilisateurice via un avertissement de sécurité) si cela n'est pas possible,
- l'empreinte de Tor browser est volontairement réduite au minimum : sur Internet,
- on peut ajouter l'extension Ublock origin sur Tor browser qui bloque la plupart des cookies malveillants à l'heure de l'écriture de ce guide (2024)[30].

Notez que de nombreux sites web bloquent l'accès à Tor à leurs services ou multiplient les captchas ce qui empêche de consulter ces sites en passant par Tor. La page d'aide du project Tor dit que la principale solution face à ces blocages est collective : faire en sorte que de nombreuxes utilisateurices contactent les hébergeurs du site web en question pour se plaindre du blocage de Tor.

D'autre part, le protocole HTTPS ne signifie pas une sécurité totale : il ne vous protège que lors du transport des informations entre vous et le site web que vous consultez[31] et de manière imparfaite. Des autorités de certification peuvent par exemple aisément falsifier des certifications HTTPS donnant une illusion de sécurité[32]. Quand cela est possible, on préfère utiliser les versions en .onion des sites afin de ne pas dépendre d'autorités extérieures. Ces sites en .onion ne sont consultables que via Tor.

Si on ne peut pas ou ne souhaite pas utiliser le navigateur Tor browser, on recommande d'utiliser le navigateur Firefox avec les extensions Ublock origin, privacy badger, decentraleyes, cookie autodelete et avec le mode https only activé.

30 Google qui contrôle Chrome et Youtube tente souvent d'empêcher les bloqueurs de pub de fonctionner convenablement.

31 https://sebsauvage.net/comprendre/ssl/ explique comment fonctionne HTTPS et ses limites.

32 La page wikipédia sur les autorités de certification explique les limites de fonctionner via un système centralisé de certifications TLS.

FBI, etc.) cherchent à lever l'anonymat que Tor procure notamment dans la lutte contre le marché noir.

De plus, le fournisseur d'accès Internet connaît vos heures d'accès à Tor ainsi que le volume de données qui transitent par Tor. Via ces éléments, on peut tenter de retrouver ce que vous avez fait sur Tor. D'où l'importance de ne pas utiliser Tor uniquement pour des activités sensibles. En faisant cela, on participe à cacher dans la masse des personnes ayant besoin de protéger leur anonymat.

4.2. Attaques spécifiques à la navigation web

Quand on navigue sur un site web, on demande à notre fournisseur d'accès Internet de communiquer avec un serveur qui stocke le site web. Ces communications peuvent contenir des données que l'on préfèrerait garder cachées. Voyons quelques exemples qui peuvent être gênants.

- Quand un site utilise uniquement le protocole HTTP au lieu du protocole HTTPS, le contenu des informations que vous consultez n'est pas chiffré[28]. Cela signifie que de nombreux acteurs d'Internet (serveurs intermédiaires, fournisseur d'accès à Internet) ont accès à ce que vous consultez. On peut imaginer l'analogie d'une carte postale qui navigue entre vous et le serveur du site web : tous les intermédiaires qui transportent la carte postale peuvent consulter le contenu de la carte.
- Quand vous consultez un site web, le navigateur communique des informations sur votre ordinateur. C'est ce qu'on appelle l'empreinte[29] du navigateur : elle contient notamment la résolution du navigateur, la version exacte du navigateur, le langage de votre navigateur, l'heure de l'ordinateur, les polices d'écritures que vous avez installées, etc. Ces informations peuvent compromettre votre anonymat pendant la navigation sur le web.
- Certains sites Internet que l'on consulte demandent au navigateur de stocker des données concernant notre navigation et que notre navigateur communique à chaque fois que l'on interagit avec le serveur du site en question. Ces données, appelées cookies, contiennent souvent un identifiant associé au navigateur. Ensuite les serveurs des sites stockent des données pour chaque identifiant comme :

28 Les navigateurs indiquent souvent un avertissement de sécurité quand on consulte une page en HTTP.

29 Vous pouvez tester votre empreinte sur le site https://coveryourtracks.eff.org/

s'introduit dans votre téléphone. Cela peut aussi être en vous envoyant un SMS avec un lien comme pour le logiciel Pegasus[19].

On peut aussi cacher les caméras des téléphones via des stickers pour éviter que quelqu'un ayant piraté votre téléphone puisse prendre des photos ou vidéos sans que vous le sachiez.

Ne pas utiliser de téléphones ou ne pas l'avoir avec soi ou l'utiliser le moins possible constituent les meilleurs méthodes de protection face à cette attaque. Encourager les collectifs militants à être moins dépendants des téléphones (messageries instantanées, etc.) constitue une défense collective efficace face à l'omniprésence des téléphones et donc de mouchards potentiels.

Cependant c'est important de se rendre compte que l'utilisation de tels outils, comme les vulnérabilités dites zero-day[20], est souvent extrêmement onéreuse.

2.4. Conclusion : le téléphone, un objet que l'on peut difficilement protéger

Comme on l'a vu avec la dernière attaque, les téléphones ne seront jamais « sécurisés ». Quoi que l'on fasse, une carte SIM active est géolocalisée régulièrement ce qui suffit pour avoir accès à une quantité impressionnante d'informations même si cette carte SIM n'est pas reliée à une identité civile (cependant elle pourra l'être plus tard si la police arrive un jour à relier les différentes identités numériques et civile).

Il vaut mieux éviter de lire ses mails sur son smartphone si on a un ordinateur accessible pour le faire suffisamment régulièrement par exemple via Tails (voir plus tard).

Les applications de messagerie instantanée via Internet permettent d'éviter la surveillance de masse via les factures détaillées de téléphonie mais absolument pas de garantir des communications privées avec d'autres gens dans le cas d'un piratage d'un téléphone présent dans la communication.

Il vaut mieux éviter d'utiliser des téléphones et en avoir le moins souvent besoin pour des activités sensibles. Un conseil basique également est de ne jamais prendre son téléphone personnel en manifestation ou en action. D'une part pour éviter le fichage

19 https://fr.wikipedia.org/wiki/Pegasus_(logiciel_espion)

20 https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day

via la géolocalisation, d'autre part votre téléphone peut être utilisé contre vous en garde à vue par les policiers.

2.5. En pratique, que faire et quel prix

On propose ici différents dispositifs matériels ainsi que leurs prix pour se donner une idée de ce qu'il est possible de faire. Pour calculer les prix, on utilisera les prix suivants (approximatifs évidemment) :

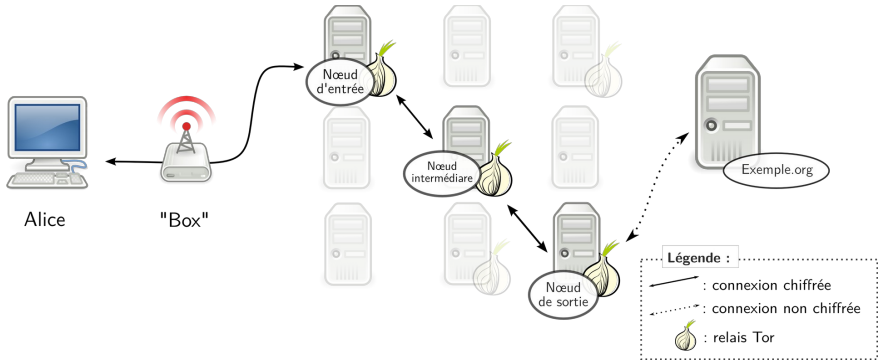
- un smartphone d'occasion coûte une cinquantaine d'euros,
- un téléphone standard coûte une dizaine d'euros.
- un abonnement 4G chez un opérateur (identité civile nécessaire) coûte approximativement 15 euros par mois.
- un abonnement 4G anonyme prépayé (Lycamobile ou Lebara) coûte 15 euros par mois. Ces abonnements peuvent s'acheter en bureaux de tabac avec du cash .

Dispositif 1 : Aucun téléphone. Prix : 0 euros
Le meilleur dispositif pour la protection numérique ! Cela sera peut-être compliqué de s'organiser avec des personnes utilisant des téléphones fréquemment.

Dispositif 2 : Un téléphone personnel uniquement. Prix : soit 50 euros + 15 euros par mois soit 10 euros + 5 euros par mois selon le format de téléphone et l'abonnement choisi.
On pourra choisir alors d'enlever sa carte SIM et si possible sa batterie avant de se rendre sur un lieu de lutte et de ne rallumer ce téléphone qu'en se déplaçant légèrement ou de manière très épisodique. Pour compartimenter les usages, on peut aussi faire attention à qui l'on donne son numéro de téléphone. En effet un numéro de téléphone avec un abonnement nominatif peut quasiment être considéré comme une pièce d'identité. Une autre option pour ce téléphone unique est de ne pas avoir d'abonnement nominatif mais uniquement des recharges de cartes prépayées sur une carte SIM liée à une identité choisie.

Dispositif 3 : Un smartphone personnel + un smartphone avec abonnement 4G anonyme. Prix : 100 euros + 30euros par mois.
Le smartphone personnel serait utilisé pour les appels familiaux et administratifs. L'autre smartphone serait pour tous les contacts que l'on s'est fait dans le milieu militant. On fera attention à ne jamais mélanger les cartes SIM entre les téléphones car sinon cela permet de fournir une identification via le numéro IMEI. On fera

Pour se protéger face à cette attaque, on conseille d'utiliser Tor. Tor essaye de faire en



Fonctionnement du réseau Tor via 3 nœuds.

sorte qu'aucun acteur autre que vous ne sache avec qui vous souhaitez communiquer en utilisant 3 nœuds qui n'ont accès qu'à des informations partielles[26].

À défaut d'utiliser Tor, on peut utiliser un VPN. Le principe est similaire sauf qu'à la place d'avoir 3 nœuds tenus par des acteurs probablement différents, il n'y a plus qu'un acteur intermédiaire entre vous et le serveur final. Cet intermédiaire a donc accès à l'intégralité de vos demandes de communication contrairement à Tor. Cependant votre fournisseur d'accès Internet sait juste que vous souhaitez communiquer avec le serveur de votre VPN.

Pour utiliser Tor pendant la navigation web, on peut installer Tor Browser sur téléphone ou ordinateur. Sur les téléphones, on peut configurer l'application Orbot pour que les autres applications passent par le réseau Tor via Orbot.

Cependant il est important de noter que la navigation Web n'est pas le seul moment où vous utilisez Internet depuis un ordinateur. En utilisant Tor Browser par exemple, vous ne protégez votre IP que pendant votre navigation mais pas le reste du temps. Le système d'exploitation Tails est pensé pour que absolument toutes les connexions à Internet passent par Tor.

Tor n'est par contre pas parfait et comporte des faiblesses[27]. Régulièrement, des attaques réussissent contre Tor car de nombreux acteurs puissants (NSA, Europol,

26 On pourra se reporter au chapitre 7 du tome 2 du guide d'autodéfense numérique pour le fonctionnement de Tor.
27 L'article wikipédia sur Tor recense une liste de limitations.

tout à fait possible. Cela peut être compliqué de bien compartimenter les usages personnels et militants dans ce cas.

Dispositif 3 : Un ordinateur + un disque dur de sauvegarde + une clé Tails + une clé Tails de sauvegarde + une clé USB de transfert de fichiers. Prix : 280 euros.
On conseille de chiffrer l'intégralité du disque dur de l'ordinateur ainsi que le disque dur. On pourra avoir deux partitions sur la clé de transfert, une chiffrée et une non-chiffrée. Avec ce dispositif, on peut bien compartimenter les usages : par exemple les usages personnels, familiaux et les achats en ligne peuvent être faits sur l'ordinateur personnel et on utilisera la clé Tails pour les usages militants.

4. Attaques spécifiques à l'utilisation d'Internet

On parlera de l'espionnage de votre utilisation d'Internet via :

- la demande des données que possède votre fournisseur d'accès Internet,
- la surveillance des communications non chiffrées,
- les trackers.

4.1. Données de notre fournisseur d'accès Internet

Quand on utilise Internet, on demande à notre fournisseur d'accès Internet de communiquer avec d'autres serveurs distants. Le fournisseur d'accès a donc connaissance de la liste des serveurs avec lesquels on communique. Cela inclut notamment :

-les serveurs des sites Web sur lesquels nous naviguons,
-les logiciels qui ont besoin d'Internet par exemple pour vérifier les mises à jour,
-les clients mails,
-les connexions ssh,
-etc.

Les autorités peuvent demander aux fournisseurs d'accès à Internet l'historique de l'utilisation d'Internet d'un abonnement.

également attention à enlever la carte SIM personnelle quand on se trouve sur un lieu de lutte et à enlever la carte SIM prépayée quand on n'est pas sur un lieu de lutte. Les deux téléphones ne devraient jamais être allumés simultanément.

On pourra aussi penser à changer de smartphone (par exemple via de l'occasion) avec abonnement 4G payé cash et avec une identité choisie et à changer de carte SIM de temps en temps histoire de brouiller les pistes.

Conseils généraux

Quand on est que de passage dans un lieu de lutte pour quelques jours, on conseille d'enlever toutes ses cartes SIM.

On peut ajouter à tout les dispositifs des téléphones standards avec recharges de 5 euros pour les actions ponctuelles (15 euros). Une fois l'action finie, on ne devrait pas réutiliser le même téléphone car le numéro IMEI a déjà été associé à une carte SIM. On pourra soit le revendre d'occasion soit s'en séparer.

3. Attaques spécifiques aux ordinateurs

On envisagera les attaques suivantes :

- tentative d'intrusion par virus,
- perquisition de l'ordinateur.

3.1. Les virus

Les virus sont des logiciels malveillants créés afin de s'introduire sur les ordinateurs et d'autres effets indésirables allant de la récupération de quelques données à la prise de contrôle totale de l'ordinateur en passant par diverses formes d'espionnage (caméra activable à distance, etc.) ou de demande de rançon pour récupérer les données (ransomware).

Pour se protéger des virus, on conseille de mettre à jour les applications dès que cela est proposé. Il s'agit souvent de mises à jour de sécurité qui protègent contre des failles que des attaquants pourraient utiliser pour entrer sur l'ordinateur[21].

Faites également attention aux documents que vous ouvrez sur votre ordinateur notamment sur Windows. Il n'est pas compliqué de mettre un virus dans un fichier PDF ou Word qui infecte votre ordinateur si vous l'ouvrez avec Acrobat ou MS

21 Par exemple, le système de chiffrement présenté ci-dessous LUKS a été mis à jour en 2023 suite à la découverte d'une faille qui aurait peut-être été utilisée par la police pour déchiffrer un disque dur. Tails a écrit un long article explicatif à ce sujet.

Office. Le code des applications libres est disponible ce qui permet à la communauté du logiciel libre de vérifier les vulnérabilités en toute transparence. Cela ne constitue cependant pas une sécurité absolue. Il y a également souvent moins d'utilisateurices des logiciels libres que des logiciels propriétaires ce qui fait qu'il y a moins d'intérêt financier à faire des virus pour ces applications.

Un antivirus à jour et un pare-feu sur Windows sont plus que nécessaires pour les utilisateur·ices de Windows. Nous ne savons pas si le pare-feu Windows présent de base sur Windows est suffisant ou s'il faut le compléter avec d'autres applications de protections.

Si votre ordinateur a une Webcam, on peut cacher la caméra avec un sticker afin qu'un utilisateur ayant pris le contrôle de notre ordinateur ne puisse pas prendre de photos ou vidéos.

3.2. Les perquisitions

Si votre ordinateur tombe dans les mains de la police et que vous n'avez rien préparé, ils auront accès à une quantité impressionnante de données sur vous. Cela va même jusqu'aux fichiers que vous avez supprimé si vous n'avez pas pensé à les écraser proprement via des applications spécifiques. Le mot de passe administrateur offre un degré de protection très faible et peut être souvent contourné.

Pour ralentir l'obtention de vos données, vous pouvez choisir de chiffrer vos données. Sur Linux, plusieurs options s'offrent à vous : Veracrypt ou Luks[22]. Attention cependant, le chiffrement des données est beaucoup plus efficace quand l'appareil est éteint[23]. Sur Windows, on peut utiliser Veracrypt pour chiffrer le disque dur. Sur Mac, FileVault 2 est un logiciel propriétaire d'Apple dont on a plus de mal à évaluer la fiabilité (vu que le code source n'est pas disponible).

La justice peut vous demander de donner vos mots de passes sous certaines conditions. Ces conditions sont difficiles à remplir et rarement remplies dans le cadre

22 Un comparatif entre Veracrypt et Luks se trouve sur le site de Tails.

23 Cela ne veut pas dire qu'il n'y a plus aucune protection quand l'appareil est allumé et déchiffré mais qu'il y a beaucoup plus d'attaques potentielles et donc que la sécurité est moindre..

de gardes à vue mais plutôt lors d'enquêtes plus longues donc **ne donnez pas vos codes** lors des gardes à vue et demandez des conseils à des legal team sinon[24]. Veracrypt permet via un système de chiffrement avec deux mots de passe (qui déverouillent des partitions de fichiers différentes) de tenter de contourner ces demandes en donnant uniquement un des deux mots de passe. L'existence d'un deuxième mot de passe et d'une deuxième partition est alors difficile à prouver.

Ne faites plus confiance à un ordinateur ou tout autre objet informatique tombé entre les mains de la police. Ils peuvent y installer des programmes espions sans que vous le sachiez. Cela peut même se faire si des personnes ont accès pendant quelques minutes à votre ordinateur sans surveillance[25]. C'est pourquoi l'on conseille de ne pas laisser traîner ses objets informatiques ou données sensibles.

L'autre danger d'une perquisition est la perte de vos données personnelles. Pour contrer cela, pensez à faire des sauvegardes que vous stockez dans des lieux sûrs et que vous actualisez régulièrement.

3.3. En pratique, que faire et quel prix

On utilisera les prix suivants pour les calculs :

- Un ordinateur portable coûte 200 euros d'occasion (prix très variable selon la gamme que l'on choisit),
- un disque dur coûte 50 euros,
- une clé USB coûte 10 euros.

Dispositif 1 : aucun ordinateur ou clé USB ou disque dur. Prix : 0 euros.
Le top en protection numérique si l'on n'utilise pas du tout Internet. Attention, emprunter l'ordinateur de quelqu'un·e d'autre pour aller sur Internet comporte des risques importants.

Dispositif 2 : Une clé USB Tails + une Clé USB Tails de sauvegarde. Prix : 20 euros
Il faudra emprunter l'ordinateur de quelqu'un·e pour utiliser sa clé Tails mais cela est

24 Un article sur Paris-luttes info datant de 2021 explique l'état des lieux juridiques sur la question des codes de téléphone en garde à vue. Il rappelle notamment qu'il y a de nombreuses conditions à remplir par la police pour que la demande des codes soit valide légalement.

25 On répertorie 4 attaques différentes si une personne malveillante a accès à votre ordinateur (même chiffré) quand vous n'êtes pas là : destruction ou vol de l'ordinateur (donc perte des données), modification mécanique de l'ordinateur pour y installer dispositifs de collecte (micro, faux clavier ,etc.), modification du BIOS (logiciels de la carte mère) et modification de la partie non chiffrée du disque dur pour y installer des logiciels malveullants (souvent la partition de boot est non chiffré).