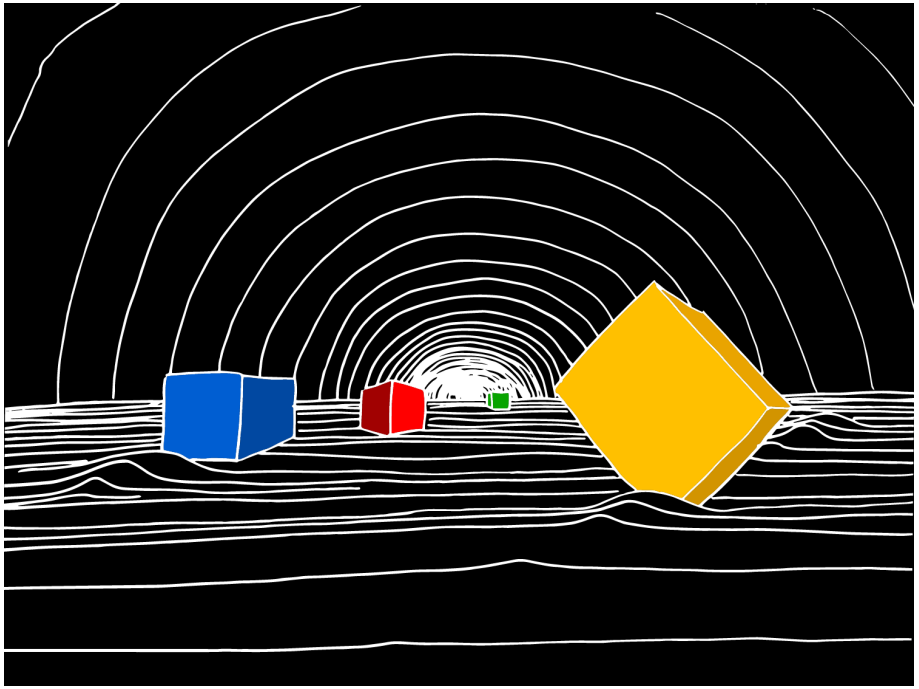
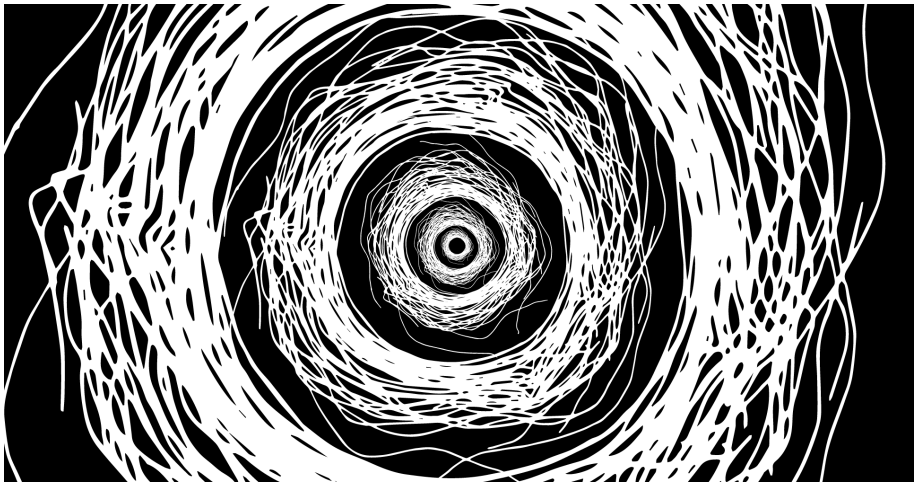
Quelles sont les principales menaces numériques et comment s'en protéger ? Comment fonctionne la surveillance numérique ? Que penser de Signal ? Des mails ? Des smartphones ? Comment gérer ses mots de passes ? Que faire des réseaux sociaux ? Ce guide de survie tente de présenter de manière synthétique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



Boîte à outils de la Zad du Carnet
Pas de Copyright. Reproduction vivement conseillée

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



Guide élaboré sur la Zad du Carnet en 2020/2021.
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.

8. Ressources utiles :

- https://tails.boum.org/home/index.fr.html Le site de Tails pour installer Tails et apprendre à l'utiliser
- https://infokiosques.net/spip.php?article1726 Le TuTORiel Tails regroupe de nombreux tutoriels très utiles
- 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://rebellyon.info/Comment-s-organiser-en-ligne-Une-brochure-22066 Une brochure qui regroupe pleins de conseils pratiques sur Comment s'organiser en ligne.
- https://zeka.noblogs.org/guide-de-protection-numerique/ est un autre guide de protection numérique.
- 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://atelier.mediaslibres.org/M-I-F-I-P-5-pratiques-de-base-pour.html est un article écrit dans la même optique que ce guide de survie.
- https://securityinabox.org/en/ regroupe de nombreux tutoriels en anglais et possède une version francaise : https://securityinabox.org/fr/
- Le site Infokiosques.net regroupe quelques brochures sur l'informatique : https://infokiosques.net/informatique
- 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 https://chatons.org/
- https://riseup.net/en/security/resources/radical-servers est une liste de serveurs politiquement engagé à travers le monde pour des services libres et décentralisés.

Crédits des images (dans l'ordre) :

1. Image de la quadrature du net
2. Logo de la Zad du Carnet CC-BY-SA 4.0
3. Représentation de la triade CIA par Ljean
4. Capture d'écran du logiciel KeepassXC
5. Image trouvée sur reddit
6. Logo de Technopolice.fr CC-BY-SA 4.0
7. Logo de Linux Unified Key Setup
8. Image extraite du guide d'autodéfense numérique
9. Image extraite d'un cours sur Dane
10. Image extraite du guide d'autodéfense numérique
11. Image de la quadrature du net
12. Logo de Tails

Atelier 2 : Installer des applications plus respectueuses de la vie privée.
Durée variable
On pense à Openstreetmap, 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, 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 flux RSS
Durée estimée : 2h

Atelier 2 : Mettre des gommettes sur les caméras des ordinateurs et téléphones que l'on utilise.
Durée estimée : 1h

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

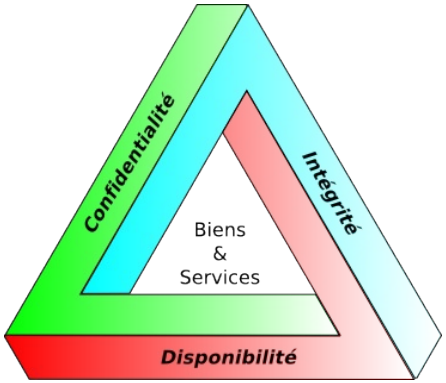
On parlera dans ce guide d'attaques pour obtenir des données numériques que l'on souhaiterait garder privées. On présentera d'abord les attaques les plus courantes, celles liées aux erreurs humaines. On parlera ensuite des attaques spécifiques aux supports physiques que l'on utilise : téléphone et ordinateur.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

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

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 protection numérique, on cherche à protéger la confidentialité, l'intégrité et la disponibilité de nos données.

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[36] regroupe de nombreux tutoriels et constitue une bonne référence pour la plupart des ateliers proposés.

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 (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 : 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 : 4h
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 fort 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 4 : Créer une clé Tails de sauvegarde.
Durée estimée : 1h

Atelier 5 : Créer de nouvelles adresses mails pour compartimenter les usages
Durée estimée : 1-3h
Il faudra peut-être trouver des invitations via des ami·es pour créer des adresses riseup. On préfèrera cependant créer des adresses sur des serveurs mails variés dans une optique de décentralisation.

Atelier 6 : Utiliser le protocole PGP pour toutes ses adresses mails
Durée estimée : 3h

Atelier 7 : Créer un disque dur de sauvegarde chiffré.
Durée estimée : variable, compter 4h (temps de copie des données peut être long).

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 : 2h

36 https://infokiosques.net/spip.php?article1726

Pour éviter d'être trop facilement espionnables, on préfèrera utiliser des applications de messagerie par Internet comme Signal, 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.

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

6.6. 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 les modules suivants : Privacy Badger, Ublock Origin, HTTPS everywhere, Cookie Autodelete.

6.7. Limiter l'utilisation des réseaux sociaux

Le mieux est évidemment de quitter les réseaux sociaux. Si cela est compliqué pour vous, limitez votre activité dessus au strict minimum. Pour aider collectivement les personnes quittant les réseaux sociaux, ne postez que des documents (articles, images, vidéos, etc.) déjà présents sur un autre support et en mettant un lien vers ce dernier.

35 Le témoignage de Julie sur Cortana recueilli par la Quadrature du Net est édifiant sur les possibilités d'espionnage offertes par les téléphones portables : https://www.laquadrature.net/2018/05/18/temoin_cortana/

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. 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[1]. 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.

1.3. La mauvaise gestion des mots de passe

Les dangers : réutilisation des mêmes mots de passe et mots de passe courts

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 courantes et il est probable qu'une de vos combinaisons identifiant et mot de passe ait déjà fuité sur le web[2].

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. Les meilleurs mots de passe sont

1 Pour plus d'informations sur la culture de la sécurité, on pourra lire une brochure de Crimethinc sur Infokiosques https://infokiosques.net/lire.php?id_article=556

2 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/

souvent ceux générés aléatoirement et qui comportent au moins 16 caractères[3]. Les gestionnaires de mots de passe (voir plus bas) proposent ce genre de fonctionnalités.

Une autre méthode facile pour retenir des mots de passe est de retenir une phrase simple comme par exemple « les chevaux aiment bien les carottes roses ». Le mot de passe est alors « chevaux carottes roses » ce qui fait 22 caractères. On peut aussi souhaiter améliorer la robustesse du mot de passe en modifiant légèrement les mots du dictionnaires. Par exemple, « chev@ux carottes r0ses » est un mot de passe plus robuste que « chevaux carottes roses ». Cependant, ce genre de mots de passe utilisant des mots du dictionnaire seront moins robustes que les mots de passe aléatoires de longueur similaire.

Les gestionnaires de mots de passe permettent de se simplifier la vie

Pour éviter d'utiliser plusieurs fois le même mot de passe et avoir des mots de passe longs, on conseille d'utiliser un gestionnaire de mot de passe et d'utiliser au maximum des mots de passe à usage unique.

Exemple d'utilisation de KeepassXC.

KeepassXC est un gestionnaire de mot de passe. Cette application peut stocker dans une base de données un grand nombre de mots de passe. Idéalement le mot de passe principal qui débloque la base de mots de passe doit être long et unique à cette base de données. Cela permet de ne pas avoir à se souvenir de tout les mots de passe à usage unique que vous utilisez, mais uniquement de celui qui permet de débloquer la base de données.

3 https://fr.wikipedia.org/wiki/Mot_de_passe#Choix_du_mot_de_passe

- le fait de passer par Tor systématiquement vous empêche parfois de vous connecter à des services que vous utilisiez d'habitude,
- surveillance considérable de Tails et attaques quelques fois réussies contre Tails[33]. Tails peut donner un faux sentiment de sécurité ce qui peut être dangereux.

Linux, plus compliqué à protéger mais plus flexible

Linux est l'autre choix naturel pour la protection numérique. Il permet de chiffrer l'intégralité de votre disque dur via le système Luks ce qui n'est pas négligeable. De plus, peu de virus existent sur Linux.

Il faudra par contre installer vous-mêmes Tor et vous y connaître un peu pour protéger votre anonymat sur Internet. Faites attention aux applications que vous installez sur Linux.

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

6.3. Faites 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[34]. 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 et préférer les mails aux échanges via téléphone

On pourra faire attention à créer plusieurs adresses mails selon les usages : personnel, militant, etc.

Les mails sont globalement plus sécurisables que les téléphones à condition d'utiliser le protocole PGP et de ne jamais consulter ses mails sur son téléphone. Ce protocole n'est pas compliqué à mettre en place. Attention cependant à ne pas perdre vos clés de chiffrement en faisant des sauvegardes dans des lieux sûrs.

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[35]. Si on prend en plus l'habitude d'enlever sa carte SIM quand on n'utilise pas son téléphone, c'est encore mieux.

33 https://tails.boum.org/doc/about/warning/index.fr.html recense de nombreuses limitations de Tails.
34 https://tails.boum.org/doc/first_steps/persistence/backup/index.en.html

6. En pratique, que faire ?

6.1. Prendre au sérieux la surveillance numérique

Ce guide n'est pas uniquement pour les militant·es aguerri·es. La surveillance numérique est principalement mise en place grâce à de grandes bases de données[30] récupérées via de nombreuses personnes y compris des personnes qui pensent n'avoir rien à cacher[31]. Ces données sont ensuite analysées par ordinateur.

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. La surveillance est un enjeu collectif et non individuel.

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[32]. 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 de vos connexions à Internet,
- les utilisateur·ices de Tails se ressemblent sur Internet ce qui procure une certaine forme d'anonymat,
- vos 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,

30 Et cette surveillance est en plein essor comme le montre l'actualité : https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/

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

32 Un tutoriel pour apprendre à utiliser Tails est disponible sur Infokiosques.net https://infokiosques.net/spip.php?article1726

Temps nécessaire à un hacker pour trouver votre mot de passe

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Diagramme donnant une idée du temps nécessaire pour trouver un mot de passe par la force brute de calcul. Les données sont vieilles de quelques années. Source : Howsecureismypassword.net.

Comme illustré ci-dessus, on préférera les mots de passe mélangeant des lettres et des chiffres à des mots de passe ne comportant que des chiffres. Cette remarque est particulièrement importante pour les codes de déverrouillage de téléphones. Préférez quand cela est possible des codes de déverrouillage avec des lettres aux codes qui ne comportent que des chiffres.

1.4. Les réseaux sociaux

La quantité d'informations que vous pouvez donner sur vous-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 vous souhaiteriez probablement garder cachées et un pouvoir considérable[4]. Les réseaux sociaux sont conçus pour se rendre indispensables et addictifs ce qui est dangereux.

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.

4 https://infokiosques.net/spip.php?article1725 pour se rendre compte de ce que peut faire Facebook avec le pouvoir qu'on lui donne en l'utilisant.

Si vous utilisez les réseaux sociaux pour vous informer, on vous conseille d'utiliser les flux RSS[5]. 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 pour ne pas exclure les militant·es qui font le choix de ne plus les utiliser[6].

Si vous aimez quand même le concept des réseaux sociaux par exemple pour rester en contact avec des ami·es, le réseau Mastodon[7] est plus respectueux de la vie privée même s'il est loin d'être exempt de certains défauts (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.

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 choses potentielles. On conseille de les supprimer systématiquement dès que l'on partage un fichier. Le système d'exploitation Tails intègre le logiciel mat2 pour supprimer les métadonnées. Ce logiciel est téléchargeable pour Linux et sinon des sites web proposent de supprimer les métadonnées pour vous via mat2[8].

5 Le site Infokiosques.net propose quelques tutoriels pour apprendre à utiliser les flux RSS https://infokiosques.net/spip.php?article794
6 https://zadducarnet.org/index.php/2020/10/30/lettre-a-celleux-qui-militent-sur-les-reseaux-sociaux/
7 https://joinmastodon.org/
8 https://metadata.systemli.org/

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 lit les e-mails transitant par ses serveurs et les fait analyser par ordinateur.

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)[25].

Un des dangers de la centralisation des adresses mails sur les mêmes serveurs par exemple riseup 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 pour notre vie personnelle, notre travail, notre activité militante est bénéfique. Sinon les autorités peuvent retrouver votre identité via votre adresse mail. On pourra aussi choisir d'avoir plusieurs adresses mails[26] 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.

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[27].

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[28]**.** On peut le faire sur Signal et Conversations en cherchant dans les paramètres. Pour le protocole PGP, on peut regarder sur les serveurs de clés et utiliser le principe de la toile de confiance[29] ou vérifier par d'autres moyens (visuellement par exemple) que l'on a les bonnes clés publiques.

25 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. Voir leur site : https://chatons.org/. Riseup recense aussi des serveurs engagés : https://riseup.net/en/security/resources/radical-servers.
26 Si vous avez une adresse mail riseup, vous pouvez créer des alias https://riseup.net/aliases
27 https://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistante
28 https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu
29 https://fr.wikipedia.org/wiki/Toile_de_confiance

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 contrôle 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.

De plus 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 pirater le serveur de Signal, ils ont donc accès aux métadonnées de toutes les conversations passant par Signal.

Dans le cas d'une application décentralisée, pour avoir accès aux métadonnées d'une conversation, il faut que les autorités piratent un serveur utilisé pour cette conversation. En piratant ce serveur, elles n'auront accès qu'aux métadonnées des utilisateur·ices de ce serveur et pas aux métadonnées d'autres conversations passant par d'autres serveurs. De plus les applications décentralisées sont moins sensibles aux attaques par déni de service[23] 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[24] 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 stockées de manière permanente sur vos appareils par exemple en activant l'option de messages éphémères disponibles sur certaines applications.

5.3. 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,l es serveurs de Riseup sont maintenus par des

23 Il semblerait que la messagerie Telegram ait été attaquée à Hong Kong en 2019 pendant les manifestations https://en.wikipedia.org/wiki/Denial-of-service_attack#Hong_Kong's_Telegram

24 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.

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 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[9]. À ce stade, 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.

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

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

Toutes les 5 minutes, votre téléphone envoie un signal aux antennes proches (qui peuvent déterminer votre position via une triangulation de 3 antennes), 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.

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[10] (le prix fixé au journal officiel 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 auxquelles un téléphone se connecte.

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

9 Pour se renseigner à ce sujet, on conseille le manuel de survie en garde à vue disponible sur infokiosques : https://infokiosques.net/spip.php?article1582

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

La facture détaillée d'un numéro de téléphone contient de nombreuses informations analysables facilement par ordinateurs. 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.**

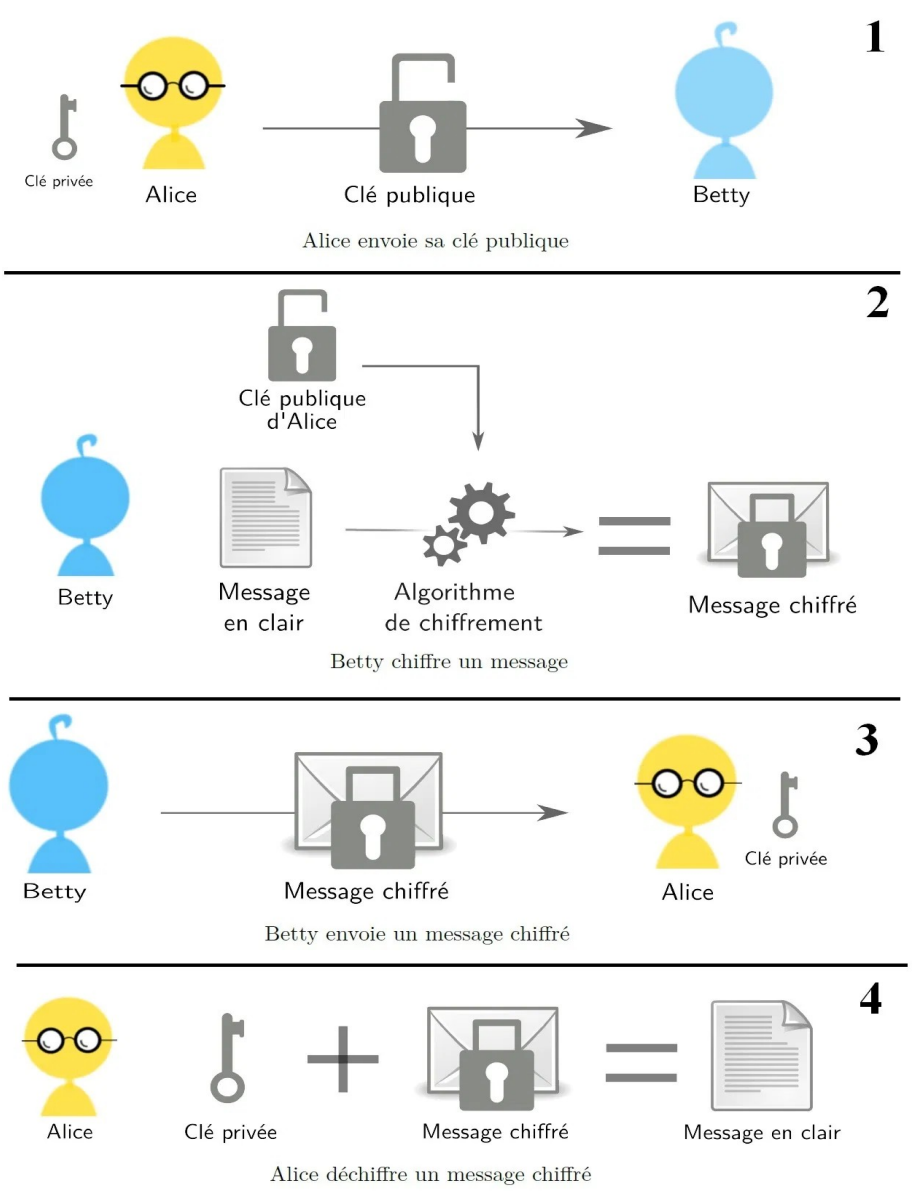
Face à la géolocalisation : cartes SIM prépayées et ne pas toujours prendre son téléphone avec soi

Il est possible d'utiliser des cartes SIM prépayées (Lebara, Lycamobile par exemple). On peut associer une fausse identité à ces cartes SIM et non sa vraie identité. Il n'empêche que votre carte SIM prépayée sera quand même géolocalisée toutes les 5 minutes. De plus, les autorités pourraient recouper votre fausse identité d'une carte SIM prépayée avec votre vraie identité civile un jour. Les prix des appels, des SMS ainsi que des données Internet des cartes SIM prépayées sont importants.

Notez bien que si vous mettez une carte SIM prépayée avec une fausse identité dans un téléphone que vous utilisiez auparavant, le numéro IMEI du téléphone reste le même. Cela permet d'établir un lien entre votre fausse identité et votre vraie identité. 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 votre fausse identité de carte SIM prépayée avec votre vraie identité, utilisez un téléphone acheté cash où vous n'avez jamais mis de cartes SIM à votre nom.

Même des solutions partielles comme les cartes SIM prépayées sous des faux noms peut considérablement compliquer le travail de la justice. Même si les services de renseignement arrivent à relier votre fausse identité à votre vraie identité, 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 si cela est possible le laisser allumer chez soi comme si on était resté à la maison.



llustration expliquant le fonctionnement du protocole PGP.

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 mieux vous protéger, y compris de vos hébergeurs d'adresse mails, on vous conseille d'utiliser le protocole PGP[20] qui est un mécanisme de chiffrement bout-à-bout que vous contrôlez. Vous n'aurez de plus plus à faire confiance aux acteurs intermédiaires pour bien chiffrer vos données vu que vous le ferez vous-mêmes.

Faites attention également aux usurpations d'identité. Il n'est pas si compliqué de se faire passer pour quelqu'un·e d'autre lors de l'envoi d'un mail. On ne peut donc pas être certain·e sans procéder à des vérifications que c'est bien la personne que vous pensez qui vous envoie un mail même si l'adresse mail semble correspondre.

Le système PGP vous protège de ces usurpations via un système de signature numérique.

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

Client mail ou webmail ?

Les clients mails comme Thunderbird, 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 ses adresses mails sur Tor Browser si le disque dur n'est pas chiffré.

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.

5.2. Signal, WhatsApp, Telegram, XMPP, Matrix

Signal, WhatsApp, Telegram, XMPP, Matrix utilisent un protocole de chiffrement bout-à-bout avec quelques spécificités selon les protocoles sur lesquels on ne s'attardera pas ici[21]. 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[22].

20 Pour plus d'infos sur comment mettre en place le protocole PGP : https://emailselfdefense.fsf.org/fr/
21 https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_protocols
22 Voir l'article du 24/05/2017 sur https://attaque.noblogs.org/files/2020/06/french_intelligence_fr.pdf

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

Enlever sa carte SIM et éteindre son téléphone régulièrement et en faire une habitude est utile.

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). Même en demandant à votre fournisseur d'accès internet votre relevé détaillé de la facture d'Internet, la police aura accès à moins de métadonnées. En effet, le fournisseur d'accès Internet 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

Chaque fois que vous installez une application, cette dernière stocke des données sur votre téléphone ainsi que sur des serveurs distants (le « cloud »). La police peut récupérer ces données par

exemple en accédant à votre téléphone via une perquisition ou en demandant aux propriétaires ou développeurs 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 votre GPS ainsi que l'historique de vos trajets,
- 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.

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.

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.

On conseille de se séparer définitivement de tout téléphone qui a passé un moment dans les mains de la police loin de votre surveillance car des mouchards peuvent y avoir été mis.

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[11] 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[12], c'est

11 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/

12 Pour plus d'information sur le mouvement du logiciel libre, on peut consulter Wikipedia : https://fr.wikipedia.org/wiki/Logiciel_libre et la carte des alternatives de Framasoft https://degooglisons-

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.

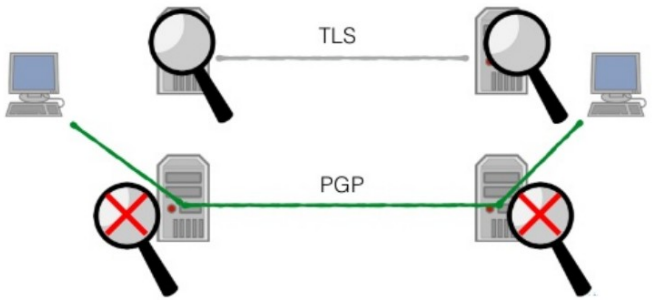
Quand un message va de Alice à Betty via Internet, des données transitent par un grand nombre de serveurs. Les systèmes de chiffrement font en sorte que ces serveurs intermédiaires ne puissent pas déchiffrer ces données en le contenu du message entre Alice et Betty.

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.

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.



Les serveurs de mails ont accès aux contenus de vos mails si vous n'utilisez que le protocole TLS (présent souvent par défaut). Cela n'est pas le cas quand vous utilisez le protocole PGP.

empreinte[19], qui peut vous identifier. Dans cette empreinte, on peut par exemple trouver la résolution de votre navigateur, la version exacte de votre navigateur, le langage de votre navigateur, l'heure de votre ordinateur, les polices d'écritures que vous avez installées, etc.

Le système d'exploitation Tails fait en sorte que cette empreinte de navigateur soit la plus standardisée possible et soit la même pour toustes les utilisateur·ices de Tails. N'hésitez pas aussi à utiliser systématiquement Tor Browser. Plus de personnes utiliseront Tor Browser, plus ce navigateur aura une empreinte générique.

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

quelques fois trouver des applications faites par des personnes luttant pour la vie privée sur Internet et contre la surveillance de masse.

Ainsi pour installer des logiciels sur Android, on recommande d'utiliser F-Droid et non le Google Play Store. De même on préférera OpenStreetMap comme application GPS, Firefox ou Tor Browser comme navigateur Web et NewPipe à l'application Youtube pour regarder des vidéos.

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.

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 que vous écrivez dans votre 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 s'introduit dans votre téléphone. Cela peut aussi être en vous envoyant un SMS avec un lien comme pour le logiciel Pegasus[13].

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.

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 toutes les 5 minutes ce qui suffit pour avoir accès à

internet.org/fr/alternatives/

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

une quantité impressionnante d'informations même si cette carte SIM n'est pas reliée à votre vraie identité (cependant elle pourra l'être plus tard si la police arrive un jour à recouper vos 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 comme Signal 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 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 coûte 60 euros,
- un téléphone standard coûte 25 euros
- un abonnement 4G chez un opérateur (identité civile nécessaire) coûte 15 euros par mois
- un abonnement 4G anonyme prépayé (Lycamobile ou Lebara) coûte 20 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 60 euros + 15 euros par mois soit 25 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.

Dispositif 3 : Un smartphone personnel + un smartphone avec abonnement 4G anonyme. Prix : 120 euros + 37,50 euros 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 également attention à enlever la carte SIM personnelle

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[17]. Régulièrement, des attaques réussissent contre Tor car de nombreux acteurs puissants (NSA, Europol, 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. Surveillance des communications non chiffrées

De nombreux sites Internet utilisent encore le protocole HTTP. Ce protocole fait que les communications entre vous et le serveur final auquel vous souhaitez accéder ne sont pas chiffrées ni pour le serveur final ni pour votre fournisseur d'accès Internet.

Si vous utilisez Tor, utilisez les sites .onion le plus souvent possible. Sinon on conseille d'utiliser le protocole HTTPS qui chiffre vos données de bout-à-bout c'est-à-dire que seuls vous et le serveur auquel vous souhaitez accéder ont accès aux données que vous demandez. Un module installable sur Firefox s'appelle HTTPS everywhere, elle force votre navigateur à utiliser le protocole HTTPS quand cela est possible.

Mais sachez que HTTPS ne vous protège que lors du transport des informations entre vous et le site web que vous consultez[18] et de manière imparfaite. Des autorités peuvent par exemple aisément falsifier des certifications HTTPS donnant une illusion de sécurité.

4.3. Trackers, cookies

Les trackers sont des données que votre navigateur Web fournit aux sites que vous souhaitez consulter qui peuvent permettre de vous identifier et de vous pister. Les cookies sont des données que votre navigateur stocke sur votre ordinateur. Ces données peuvent être le fait que vous avez choisi de rester authentifié plusieurs jours sur tel site, les vidéos que vous avez regardées, les marchandises que vous avez regardées sur un site d'achat en ligne, etc. Certains cookies sont des cookies dits de pistage et sont mis par des sites malveillants pour analyser vos habitudes de visite et d'achats en lignes.

Pour vous protéger des cookies malveillants entre autres, on conseille d'installer Privacy Badger, uBlock Origin et Cookie Autodelete sur votre navigateur Firefox. Pensez aussi à mettre les paramètres de confidentialité au maximum et d'être tout le temps en navigation privée.

Mais les cookies malveillants ne sont pas la seule méthode de pistage. Quand vous communiquez avec un site Web, vous communiquez un ensemble d'informations sur votre navigateur, une

17 https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Weaknesses
18 https://sebsauvage.net/comprendre/ssl/

4. Attaques spécifiques à la navigation Web

On parlera de l'espionnage de votre navigation Web via :

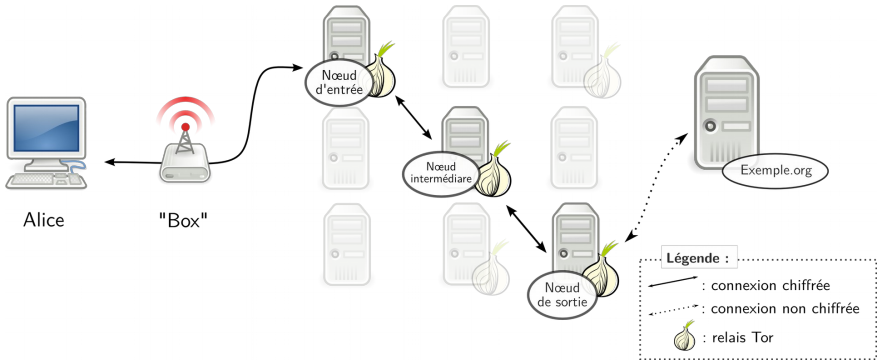
- la demande des données que possède votre fournisseur d'accès Internet

- la surveillance des communications non chiffrées,

- les trackers.

4.1. Données de votre fournisseur d'accès Internet

Quand vous naviguez sur le Web, vous demandez à votre fournisseur d'accès Internet de communiquer avec les serveurs qui gèrent les sites Web que vous visitez. Ce dernier peut donc savoir quels sites vous consultez, ce que vous y faites et stocke ces données. Les autorités peuvent demander à votre fournisseur d'accès Internet l'historique de votre utilisation d'Internet et donc de votre navigation Web en particulier.



Fonctionnement du réseau Tor via 3 nœuds.

Pour se protéger face à cette attaque, on conseille d'utiliser Tor. Le principe de Tor est très simple, il essaye de faire en sorte qu'aucun serveur ne sache avec qui vous souhaitez communiquer en utilisant 3 nœuds qui n'ont accès qu'à des informations partielles[16].

À défaut d'utiliser Tor, vous pouvez utiliser un VPN. Le principe est similaire sauf qu'à la place d'avoir 3 nœuds tenus par des acteurs probablement différents, vous n'avez 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, 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.

16 On pourra se reporter au chapitre 7 du tome 2 du guide d'autodéfense numérique pour le fonctionnement de Tor.

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

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 (30 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 peuvent s'introduire sur votre ordinateur pour des effets indésirables allant de la récupération de quelques données à la prise de contrôle totale de votre ordinateur en passant par diverses formes d'espionnage (caméra activable à distance, etc.) ou de demande de rançon pour récupérer vos données (ransomware).

Pour vous protéger des virus, on vous conseille de mettre à jour vos applications dès que l'on vous le propose. Il s'agit souvent de mises à jour de sécurité qui vous protègent contre des failles que des attaquants pourraient utiliser pour entrer sur votre ordinateur.

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 Office. Les applications libres sous Linux comme LibreOffice sont plus résistantes face à ce type d'attaques principalement car il y a moins d'intérêt financier à faire des virus pour Linux. Cela n'empêche pas une attaque ciblée contre une personne utilisant Linux.

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 d'un mac ou d'un Windows ne vous protège absolument pas et le choisir long ne servira qu'à vous protéger d'ami·es intrusif·ves n'ayant pas le temps de se renseigner pour les contourner.

Pour ralentir l'obtention de vos données, vous pouvez choisir de chiffrer vos données. Plusieurs options s'offrent à vous : Veracrypt ou Luks[14]. Attention cependant, vous ne pourrez faire confiance au chiffrement de vos données via Luks ou Veracrypt que si votre ordinateur est éteint.

Toutefois si la justice vous présente une demande de vos mots de passes ou clés de chiffrement, vous êtes tenu·es de les donner et vous encourez une peine maximum de 3 ans d'emprisonnement et 270 000 euros d'amende en cas de refus. Ces demandes ne sont que rarement effectuées dans le cadre de gardes à vue mais plutôt lors d'enquêtes plus longues donc ne donnez pas vos codes lors des gardes à vue[15]. Veracrypt permet via un système de chiffrement avec deux mots de passe (un vrai et un faux) de tenter de contourner ces demandes en donnant uniquement le faux mot de passe.

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. Un système d'exploitation sur une clé USB comme Tails peut être plus facilement protégé qu'un ordinateur car facilement transportable sur vous à tout moment.

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 400 euros (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 est dangereux.

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 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 : 480 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.

14 Un comparatif entre Veracrypt et Luks se trouve ici : https://tails.boum.org/doc/encryption_and_privacy/luks_vs_veracrypt.inline/index.en.html

15 https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018?lang=fr explique l'état des lieux juridiques sur la question des codes de téléphone en garde à vue.