Comment se protéger et protéger nos luttes

-Premiers pas dans la mise en place de pratiques de sécurité-

Elle a été écrite en 2023.
Si vous voulez nous contacter : *brochure-secu@riseup.net*

Sommaire

Introduction

Cette brochure est une introduction à la culture de sécurité ainsi qu'à certains outils numériques.

Elle a été écrite par des personnes ayant une petite expérience militante et une connaissance, parfois limitée, dans le domaine de l'informatique. L'idée n'était pas d'écrire un manuel pointu, non non non, mais plutôt d'offrir la possibilité aux personnes n'y connaissant rien de mettre un premier (ou un deuxième!) pied dans ces sujets nébuleux.

Elle se base sur des formations qu'on a pu recevoir ou donner, sur notre expérience personnelle, sur des échanges nombreux avec des personnes concernées, mais aussi sur une bonne grosse bibliographie.

Elle s'adresse principalement aux militant·es de tous poils, mais elle peut être utile pour toute personne s'interrogeant sur la protection de sa vie privée ou de celle de son entourage.

Outre proposer des apports théoriques et des pistes de réflexions, elle a aussi été créée dans l'optique de servir de support de formation pour des gens qui aimeraient transmettre ces connaissances et compétences à des pair·es.

Elle est donc construite en 4 grosses parties :

- Une première partie autour de grands principes de la culture de sécurité ainsi que l'exploration de possibles pratiques de sécurité (en évitant volontairement de parler d'informatique).
- Les outils informatiques font l'objet d'une deuxième grande partie, explorant la théorie comme la pratique.
- Elle est suivie d'annexes et propose notamment des outils pratiques, des pistes pour aller plus loin ainsi qu'un déroulé de formation, qu'on a voulu créer quasiment clé en main. Ce déroulé de formation est une proposition à remodeler selon vos contextes, vos besoins, envies, possibilités ... Elle est faite pour être bidouillée !
- La dernière partie, c'est la bibliographie, triée par thèmes et avec un petit échantillon de ce qui nous a particulièrement servi et plu pendant la rédaction de la brochure.

D'OÙ SORT CETTE BROCHURE?

Cette brochure est née d'un double constat :

☛ La répression est de plus en plus forte contre les milieux militants de gauche[1][2][3][4], et de manière générale les outils numériques de contrôle sont de plus en plus véner[5][6][7][8].

On a envie de lutter contre la répression, à la fois pour que les luttes puissent perdurer et pour prendre soin de nous, collectivement et individuellement. Autrement dit ça nous semble important de mettre en place des bonnes pratiques de sécurité parce que ça nous permet de pérenniser nos activités, ça permet à nos combats de durer dans le temps, d'être moins mis à mal par la répression. En même temps, c'est important parce que ça nous protège d'éventuels évènements difficiles psychologiquement, physiquement, émotionnellement... Par exemple, c'est cool de ne pas se retrouver en prison : à la fois parce qu'on est moins efficace quand on est en prison mais aussi parce que c'est -et c'est rien de le dire- un moment pas très agréable[9][10][11]...

☛ Les orga collectives auxquelles nous participons de près ou de loin peinent à prendre en main les enjeux de la répression et à se protéger efficacement. On sent un manque de connaissances, de compétences, d'envie et d'espaces pour se saisir des questions d'anti-répression, de mise en place de pratiques de sécurité.

Face à ce double constat on est quelques un·es à s'être motivé·es et on a décidé d'écrire cette brochure. On n'est pas des expert·es, ni dans le domaine de l'anti-répression, ni dans la mise en place de pratiques de sécurité, ni en informatique (ni en écriture de brochure d'ailleurs...) mais on a quelques compétences, connaissances qu'on nous a transmises et qu'on avait envie de retransmettre. En conséquences n'hésitez pas à aller consulter nos sources et à vous questionner sur ce qu'on vous dit, à vérifier les informations qu'on avance[12]!

---

1 https://bastamag.net/webdocs/police/ *Morts à la suite d'interventions policières*, Bastamag, 2020 (Conclusion)
2 https://www.acatfrance.fr/public/rapport_violences_policieres_acat.pdf *L'ordre et la Force - Enquête sur l'usage de la force par les représentants de la loi en France*, ACAT (Action des Chrétiens pour l'Abolition de la Torture), 2015
3 https://fr.wikipedia.org/wiki/Violence_polici%C3%A8re_en_France *Violences policières en France*, Wikipédia
4 https://www.interieur.gouv.fr/Publications/Rapports-de-l-IGPN/Rapport-annuel-d-activite-de-l-IGPN-2020 *Rapport de l'IGPN*, 2020 (p 46-47)
5 https://infokiosques.net/lire.php?id_article=1849 *Guide de survie en protection numérique à l'usage des militant·es*, 2021
6 https://www.laquadrature.net/2021/04/16/loi-securite-globale-adoptee-resumons/ *Loi sécurité globale adoptée : résumons*, La Quadrature du Net, 2021
7 https://www.laquadrature.net/2021/09/22/reglement-ia-la-commission-europeenne-tend-le-piege-de-la-reconnaissance-faciale/ *Règlement IA : la Commission européenne tend le piège de la reconnaissance faciale*, La Quadrature du Net, 2021
8 https://technopolice.be/presse/pistage-dans-le-cyberespace/ *Pistage dans le cyberespace*, Technopolice Bruxelles, 2021
9 https://infokiosques.net/lire.php?id_article=1673 *Paroles d'enfermés*, 2018
10 https://lenvolee.net/category/actualite_de_la_prison/lettres_de_prison/ *Lettres de prison*, L'Envolée
11 https://infokiosques.net/spip.php?article856 *Comme un chien enragé - Lettre anonyme d'un détenu de la prison de la Santé sur les conditions de détention et sur la prison en général*, 2011
12 https://cortecs.org/ Site internet (très riche!) du CORTECS (collectif de recherche et de transmission de l'esprit critique)

Nos Objectifs

En rédigeant cette brochure on s'est donné·es différents objectifs:

↦ Visibiliser les enjeux de sécurité. En faire une question plus centrale, qu'on se pose plus souvent notamment lorsqu'on a des activités militantes.

↦ S'autonomiser sur nos utilisations de l'informatique. Ouvrir la boîte noire de l'informatique. Casser les barrières qu'on peut se mettre à l'idée d'approcher les questions numériques : « C'est trop technique, j'y comprends rien... »

↦ Expliciter comment peut se faire le choix d'utiliser tel ou tel outil numérique et aiguiser notre esprit critique sur le choix des outils. Partager et diffuser des outils qui nous paraissaient pertinents dans des contextes courants.

↦ Favoriser la transmission de connaissances/compétences entre pair·es.

Tout ça est englobé par un objectif général qui est de diffuser, consolider, mettre en place une culture de sécurité afin de limiter la répression au niveau individuel et collectif.

Attention

Lutter pour changer la manière dont notre monde fonctionne peut se faire de multiples manières tant dans les problématiques abordées que dans la forme d'organisation ou que dans les modes d'actions, etc. On a envie de rendre hommage à toutes ces manières de lutter comme pouvant s'articuler entre elles, être allié·es[13] [14] [15]. Parfois on parle d'un 'nous' général, des 'milieux militants', parfois on prend des exemples précis. Tout ça peut avoir un effet uniformisant, et masquer toute la diversité d'actions et d'organisations qui existe. On essaye d'être vigilant·es à inclure toute cette diversité, mais sentez vous libre de prendre ou laisser ce qu'on dit par rapport à votre propre réalité.

Par ailleurs, une bonne partie des pratiques de sécurité dont on parle dans cette brochure intègre les outils numériques. Et ces outils ne sont pas neutres, ne serait-ce que dans la manière dont ils sont conçus et par qui ils le sont[16] [17]. De plus ils sont très utiles à la répression[18] [19] [20].

---

13 *Lutter Ensemble - Pour de nouvelles complicités politiques*, Juliette Rousseau, 2018

14 *Full Spectrum Resistance : Se battre et Gagner*, Aric McBay, 2019

15 https://la-maraude.fr/site/wp-content/uploads/2020/12/Mettre-fin-aE%CC%8C-lessentialisme.pdf *Mettre fin à l'essentialisme : de l'en-dedans, de l'en-dehors et de l'en-contre*, Aviv & Thomas, 2017 (p 1 à 4 surtout)

16 https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica *Scandale Facebook-Cambridge Analytica*, Wikipedia

17 https://www.brut.media/fr/science-and-technology/les-algorithmes-sont-ils-racistes-et-sexistes--6d05ba2a-d7b8-4051-b8ba-c88ec1ef987b *Les algorithmes sont-ils racistes et sexistes ?*, Brut, 2020 (article pas très intéressant, mais qui illustre bien le propos...)

18 https://infokiosques.net/lire.php?id_article=1849 *Guide de survie en protection numérique à l'usage des militant·es*, 2021

19 https://www.laquadrature.net/2021/04/16/loi-securite-globale-adoptee-resumons/ *Loi sécurité globale adoptée : résumons*, La Quadrature du Net, 2021

20 https://www.laquadrature.net/2021/09/22/reglement-ia-la-commission-europeenne-tend-le-piege-de-la-reconnaissance-faciale/ *Règlement IA* , La Quadrature du Net, 2021

Pourtant, s'en séparer ne permet pas de s'en protéger (même si je n'utilise plus de téléphone portable et d'ordinateur, l'état continue à installer des caméras de surveillance et me filmer, la police utilise des outils numériques de fichage de plus en plus efficaces, potentiellement me suspecte si je n'utilise pas certains outils :téléphone portable, carte bleue, etc.)[21] [22]. Les utiliser permet la plupart du temps de gagner en efficacité quand on s'organise à plusieurs. Cependant, ne pas les connaître peut vraiment nous mettre en danger.

De plus, cette brochure présente une partie des enjeux liés à la mise en place de pratiques de sécurité mais beaucoup de choses n'y sont pas ou peu abordées : c'est le cas notamment des TÉLÉPHONES. Nous sommes conscient·es que c'est un outil très utilisé, dans les milieux militants comme ailleurs, et que c'est une source d'information centrale pour la police et la justice[23]. Cependant, faute de temps, de place et de connaissances, on le fait pas ici. D'autres gens se sont déjà saisis de cet enjeu[24] [25], on espère que d'autres encore s'en saisiront elleux aussi et que des bonnes pratiques de sécurité autour des téléphones continueront à se diffuser.

Voilà, bonne lecture!

21 https://technopolice.fr/presentation/ site de Technopolice France

22 https://bibliothequelibertad.noblogs.org/post/2022/04/02/un-micro-trouve-a-la-bibliotheque-anarchiste-libertad *Un micro de flics trouvé à la bibliothèque anarchiste Libertad*, Libertad, 2022

23 https://blogs.mediapart.fr/louise-fessard/blog/260312/ecoutes-ce-que-la-police-peut-obtenir-des-operateurs *Ecoutes : ce que la police peut obtenir des opérateurs* Médiapart, 2012 (article parmi d'autres, mais qu'on trouvait intéressement chiffré!)

24 https://infokiosques.net/spip.php?article1975 *Téléphonie mobile : Surveillances, répressions, réduction des risques*, 2023 (brochure bien complète et très cool!)
https://infokiosques.net/lire.php?id_article=1849 *Guide de survie en protection numérique à l'usage des militant·es*, 2021

25 http://aka3xvhiygnchpsbrilphkzbdxtvr6j6pc7hluf6mf2ddruttsikswad.onion/fr/index.html#investigations-et-telephonie-mobile (en .onion) ou
https://www.csrc.link/fr/#investigations-et-telephonie-mobile *Investigations & téléphonie mobile : le guide à l'usage des avocats*, 2021

DÉFINITIONS

Sécurité

Définir la sécurité pourrait prendre beaucoup de temps. C'est un concept vaste, qui recoupe des imaginaires assez hétéroclites. On pourrait écrire des pages et des pages pour expliquer les différentes utilisations du terme, les théories (politiques mais aussi psychologiques, médicales...) qui lui sont associées, les idées auxquelles ça renvoie... On a l'impression que cette brochure c'est pas l'espace pour faire ça mais on avait quand même envie de dire quelques mots sur la manière dont on appréhende ce mot.

Déjà, le mot sécurité est un mot un peu ambivalent, qui renvoie souvent au concept d'insécurité développé par la droite[26] (et le PS[27]) (et le PCF[28]) ces dernières dizaines d'années[29]. C'est une manière de cultiver un sentiment de sécurité qui est largement contestable. Mais on a l'impression qu'on a besoin de se sentir un minimum en sécurité pour pouvoir s'épanouir, déployer des activités et construire des dynamiques, qu'elles soient collectives ou individuelles[30].

Culture de sécurité

Dans cette brochure, on parlera de culture de sécurité pour désigner la mise en place de pratiques qui, sur le long terme, permettent de renforcer sa sécurité et de se sentir plus préparé.es face aux attaques qu'on peut subir : avoir une bonne culture de sécurité c'est une manière de se pérenniser en intégrant dans nos modes de vies les enjeux de la répression. De se pérenniser et de se protéger en tant que personne[31] (éviter de se retrouver traumatisé·e après une garde-à-vue difficile qu'on aurait pu empêcher par exemple) mais aussi protéger et pérenniser ses activités, pour éviter que tout un réseau ou toute une lutte s'affaiblisse face aux assauts de la répression[32] [33].

---

26 https://www.liberation.fr/politique/securite-la-droite-na-donc-rien-dautre-a-dire-20210716_SQYZQ54GLREWJEFIKSKPQOV55I/ *Sécurité : La droite n'a donc rien d'autre à dire?*, article de Libération, 2021

27 https://www.radiofrance.fr/franceculture/podcasts/du-grain-a-moudre/securite-la-gauche-court-elle-apres-la-droite-3241327 Du grain à Moudre, *Sécurité : La gauche court-elle après la droite ?* Émission de France Culture, février 2011 (en soi c'est un débat politicard tout pourri entre Rebsamen et Ciotti, mais c'est intéressant de voir jusqu'où ils sont d'accord)

28 https://infokiosques.net/spip.php?page=lire&id_article=155 *Le mythe de l'insécurité*, 2004

29 https://www.lemondepolitique.fr/dossiers/securite-et-liberte#sidenote-18 *Sécurité et liberté*, dossier du Monde Politique, non daté (post 2015) (on sait pas trop d'où sort ce dossier et qui c'est 'le monde politique', mais ce dossier est cool)

30 https://holistic-security.tacticaltech.org/ , *Holistic security*, Tactical Technology Collective

31 https://noussommestousdesmalfaiteurs.noblogs.org/files/2021/05/SLIP_OK.cleaned.pdf ou https://noussommestousdesmalfaiteurs.noblogs.org/rendez-moi-mon-slip-la-version-integrale/ *Rendez-moi mon slip*, témoignages de la répression à Bure, 2021

32 https://mininginjustice.org/infiltration/ *Damage Control, the story of how one activist group kept ourselves safe and strong in the face of movement infiltration*, 2017 (C'est en anglais)

Une étape importante dans l'approfondissement d'une culture de de sécurité consiste à faire un « modèle de menace », ou « plan de sécurisation[34] » (ou autres noms). C'est un terme un peu compliqué qui recouvre l'idée de prendre un moment pour se poser quelques questions avant d'agir. Notamment 'que dois-je protéger? Contre qui? Quels moyens peuvent-iels mobiliser? Quelles seraient les conséquences s'iels arrivaient à accéder à ce que je cherche à protéger? Quels moyens suis-je/sommes-nous prêt·e/s à mettre en oeuvre?'. Les réponses à ses questions amèneront des stratégies et donc des pratiques de sécurité différentes selon les contextes, personnes, groupes, ...

Il est important de prendre du temps pour faire ça individuellement et au sein de nos groupes, car les réponses ne sont pas les mêmes selon qui parle. Prendre du temps permet de mettre du soin dans ce moment, y mettre de l'écoute et de la bienveillance, car c'est aussi un travail dans lequel on définit nos limites individuelles et collectives. Et il est toujours bon de rappeler que le consentement, c'est important...

Dans la suite de cette brochure, nous nous basons sur un exemple de modèle de menace que nous esquissons dans les paragraphes suivants. Ce modèle de menace est volontairement large et imprécis pour pouvoir amener plus d'éléments à la réflexion, mais il est important que vous réfléchissiez à votre propre modèle de menace afin de choisir au mieux la stratégie que vous voulez adopter et les pratiques de sécurité qui vous semblent adaptées aux situations dans lesquelles vous êtes. Ne partez pas du principe que le modèle de menace que nous évoquons est le même que le vôtre, que les risques dont nous parlons vous concerne ou que nous citons tous les risques qui peuvent être liés à votre activité.

DE QUI SE PROTÉGER

Ceci est une liste non exhaustive d'institutions ou de groupes recouvrant certes un très large spectre de ce que la répression peut compter de visages différents, mais qui reste à adapter selon les contextes et les pratiques[35].

- La police (au travers de la répression physique et administrative, légale ou non)
- La justice (au travers de la répression légale, de l'enfermement)
- Des groupes politiques opposés (fachos, voisins vigilants, etc.)
- L'administration (CAF, fac, Pôle emploi, etc.)
- L'entourage (famille, ami·x·s, voisaines, collègues, patron·nes, ...) qui peut par exemple faire subir des violences conjugales, du harcèlement au travail, de la domination d'adultes sur des enfants, etc.)
- Des entreprises, groupes d'intérêt privés, mafias...[36]

33 https://reporterre.net/A-Grenoble-six-militants-ecolos-face-a-une-justice-kafkaienne *À Grenoble, six militants écolos face à une justice kafkaïenne*, Reporterre, 2020

34 Ce terme vient du site de la Boussole, où est proposée une manière de faire ce plan de sécurisation, mais orienté numérique. https://laboussole.coop/2021/11/22/document-modele-etablir-un-plan-de-securite-informatique/

35 Source orale, entendue lors d'une formation sécu reçue en 2020 par certain·e·s des auteurices

36 https://www.mediapart.fr/journal/france/150720/l-air-libre-le-squale-operations-secretes Émission A l'air libre, *Le Squale, opérations secrètes*, Médiapart, 2020

La police, la justice ou les entreprises ont des moyens d'actions colossaux et font la plupart du temps système, c'est à dire travaillent les unes avec les autres[37] [38].

Ce sont également des institutions dominantes, qui ont une légitimité et une emprise assez globale. Les luttes militantes s'inscrivent dans un contexte de rapport de force asymétrique, le principal outil à disposition de ces institutions pour empêcher leurs opposant·es d'agir étant la répression, spécifique à ce contexte asymétrique. Elle consiste en un ensemble de pratiques : brutaliser physiquement en manif, assigner à résidence, mettre des amendes, envoyer en prison... Contrairement à une opposition symétrique, comme par exemple un champ de bataille médiéval où deux armées se font face, où les moyens d'actions sont sensiblement les mêmes et où l'ennemi est clairement identifié, ici un enjeu principal pour ces institutions est l'identification et la compréhension des objectifs, des stratégies, des manières de lutter des militant·es[39].

La répression intègre entre autres des pratiques qui aident à cette identification et compréhension : le fichage et la surveillance. Ces deux formes d'actions visent à récolter des informations. La surveillance recouvre plein de pratiques (écoutes téléphoniques, accès aux données de localisation, filatures, ...), et le fichage consiste à rassembler toutes ces infos dans des fichiers qui seront accessibles par plusieurs des acteurices dont on fait la liste ci-dessus. Cette collecte peut se faire à différentes échelles: sur une personne, un réseau ou toute une population, sur quelques semaines ou quelques dizaines d'années, ...[40]

QUI PROTÉGER

La répression ne touche pas uniquement les personnes participant à des actions illégales. Elle peut très vite toucher des gens identifiés comme militants (même s'ielles n'ont pas organisé ou participé à des actions), ainsi que leur entourage.

Un très bon exemple de ça, c'est l'affaire des 7 antifas de Lyon[41] [42] :

> *En août 2020 dans une manifestation anti-pass sanitaire, plusieurs personnes interviennent contre des gens de Civitas (mouvement d'extrême-droite) qui venaient pour se battre. Malgré le refus de porter plainte des militants de Civitas, le parquet de Lyon a décidé d'accuser 7 personnes identifiées comme antifasciste d'avoir porté des coups aux militants d'extrême-droite. Dans le cadre de l'enquête, leurs domiciles ont été perquisitionnés, le logement de l'amie d'une de ces 7 personnes aussi (pour rappel, dans une perquisition il peut notamment y avoir des affaires personnelles saisies (ordi, téléphone, agendas, etc.))*

37 https://infokiosques.net/IMG/pdf/Le_renseignement_francais-35p-fil-juin2020.pdf *Le renseignement français 2013-2020*

38 https://earsandeyes.noblogs.org/fr/industrie-surveillance-vue-d-ensemble/ *Une vue d'ensemble de l'industrie de la surveillance*, non daté.

39 https://reporterre.net/1-3-La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure *1/3 - La justice a massivement surveillé les militants antinucléaires de Bure*, Médiapart et Reporterre, 2020

40 https://rebellyon.info/La-folle-volonte-de-tout-controler-MaJ-et-23573 *La folle volonté de tout contrôler*, 2021 (85 fichiers de surveillance et de fichage passés au crible)

41 https://www.franceculture.fr/emissions/les-pieds-sur-terre/l-affaire-des-sept-antifas-a-lyon *L'affaire des sept antifas à Lyon*, Les pieds sur Terre, 2020 (interview de plusieurs personnes concernées)

42 https://www.rue89lyon.fr/2021/11/05/proces-sept-antifas-lyon/ *Le procès de sept antifas à Lyon : récit d'une affaire bancale*, 2021

Même si on ne pense pas soi-même être une victime potentielle de la répression, on peut vouloir mettre en place des pratiques de sécurité. Peut-être que des gens dans notre entourage ont des activités militantes à protéger, même s'iels ne nous l'ont pas dit. Et au-delà de ça, un truc important pour nous : en mettant en place des pratiques de sécurité, on contribue aussi à protéger des militant·es plus éloigné·es de notre entourage. Parce que plus on est nombreux·ses à mettre en place ces pratiques de sécurité moins ces pratiques sont suspectes et nous exposent à de la répression. C'est une manière de prendre soin de personnes alliées qui ne sont pas forcément dans notre entourage proche.

La petite parenthèse : Au-delà de la répression, l'utilisation d'Internet, omniprésente aujourd'hui[43], expose tout le monde à du fichage et de la surveillance. Des entreprises comme Google, Facebook, Amazon, etc. tirent une grosse partie si ce n'est la totalité de leur revenus[44] de l'utilisation du fichage et de la surveillance pour notamment construire des publicités plus efficaces[45]. Certaines personnes mettent en place des pratiques de sécurité pour lutter contre ce fonctionnement et pas spécialement pour se protéger de la répression (on développe un peu plus cette idée dans la partie sur l'informatique, *Protéger les informations qui sont sur mon disque dur, ma clé usb*, dans le paragraphe sur les logiciels de « surveillance »). Fin de la petite parenthèse.

QUOI PROTÉGER

La répression peut toucher de nombreux aspects de nos vie et s'en protéger peut impliquer d'acquérir des compétences et connaissances diverses, de se former dans de nombreux domaines: Comment se passe une garde à vue, un interrogatoire ? Comment réagir à une intervention des flics en manif ? Comment s'assurer de sa sécurité physique dans ce genre de situation ? Parmi tous les enjeux de protection face à la répression, cette brochure adresse en particulier la question de la sécurité liée aux informations.

Traces

Avant de réfléchir aux enjeux de sécurité liés aux informations, on peut déjà se poser la question suivantes : quelles informations sur moi sont disponibles, visibles et/ou enregistrables par des personnes tierces? Dans notre vie de tous les jours, on laisse ou on donne des informations un peu tous le temps et partout, des informations qui pourraient être récupérées par d'autres personnes : des *traces*. Par exemple quand je fais un paiement en ligne, que je

43 https://linc.cnil.fr/fr/barometre-du-numerique-2021-les-chiffres-des-usages-numeriques-en-france *Baromètre du numérique 2021 – Les chiffres des usages numériques en France* , Laboratoire d'Innovation Numérique de la CNIL, 2021

44 · https://www.visualcapitalist.com/wp-content/uploads/2022/09/Alphabet-Revenue-June-2022-full-size.html diagramme des revenus de Google du 3e quart de l'année 2022 ;
· https://mamot.fr/system/cache/media_attachments/files/109/252/822/452/160/647/original/57f6221c34c36444.jpg diagramme des revenus de Facebook du 3e quart de l'année 2022. (c'est en anglais, et ça vient d'un site nul. Mais bon, c'est intéressant à voir, quand même)

45 https://comptoir.org/2016/10/28/philippe-vion-dury-le-vrai-visage-de-la-silicon-valley-cest-celui-du-capitalisme-predateur/ *Le vrai visage de la Silicon Valley, c'est celui du capitalisme prédateur,* Le Comptoir, 2016

prend les transports en commun, que j'envoie un sms... c'est autant de traces, d'informations qui peuvent être récupérées et utilisées par des personnes ou des organisations.

Toutes ces informations laissées ne sont pas forcément sensibles, certaines traces sont même pertinentes. Par exemple ça peut être utile pour une bibliothèque d'avoir le contact de la personne qui a emprunté tel ouvrage, pour pouvoir lui demander de rendre le bouquin si quelqu'un·e d'autre veut le consulter. L'important est de prendre conscience des différentes traces qu'on laisse pour pouvoir se poser la question de si on a envie ou pas de les laisser.

Informations sensibles

Une fois qu'on a conscience des différentes informations éventuellement disponibles et utilisables par des personnes tierces ou des organisations, on peut se questionner : parmi ces informations, quelles informations doit-on protéger ? Autrement dit, qu'est ce qu'une information sensible?

Une réponse possible, c'est que c'est une information qui peut intéresser des ennemis politiques et/ou qui peut nous mettre en danger. On a une idée de quelles infos sont utiles à la police et à la justice aujourd'hui parce qu'on a une idée de ce qu'elles récoltent et utilisent dans les procès, par exemple[46].

Déterminer si une information est sensible ou pas est complètement dépendant du contexte, de la personne, etc. Mais dans beaucoup de cas on peut considérer deux types d'informations potentiellement sensibles : les informations liées à l'identification (identité civile, réseau, parcours) et les informations liées à une action (lieu, date, cible, ...)[47].

Par ailleurs, une fois récoltée, une information est possiblement stockée pour toujours. Lorsqu'on essaie de déterminer si une information est sensible ou non, il faut garder à l'esprit qu'une information non sensible aujourd'hui peut le devenir plus tard. Par exemple, en cas d'évolution des systèmes politiques, une activité jusque là légale et non-répréhensible peut devenir le point de départ d'une répression plus ou moins poussée[48].

---

46 https://reporterre.net/1-3-La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure *1/3 - La justice a massivement surveillé les militants antinucléaires de Bure,* Médiapart et Reporterre, 2020 ; https://reporterre.net/2-3-L-Etat-a-depense-un-million-d-euros-contre-les-antinucleaires-de-Bure *2/3 - L'État a dépensé un million d'euros contre les anti-nucléaires de Bure,* Médiapart et Reporterre, 2020 ; https://reporterre.net/A-Bure-la-justice-a-bafoue-les-droits-de-la-defense *3/3 - À Bure la justice a bafoué les droits de la défense,* Médiapart et Reporterre, 2020

47 Voir l'épisode 1/3 de l'enquête sur Bure ci-dessus.

48 « *Pendant l'occupation allemande en France, en zone libre, des personnes ont été enfermées pour 'activités communistes'. Certaines de ces personnes étaient des élus municipaux communistes avant la guerre. Pas très difficile de les identifier...* » retour issu d'une discussion orale avec un chercheur en histoire.

PISTES DE RÉFLEXIONS SUR LA MISE EN PLACE DE PRATIQUES DE SÉCURITÉ

QUESTIONNEMENTS

Avec tout ce qui a été amené, on en vient à se poser plusieurs questions, et notamment : Comment intégrer la culture de sécurité dans notre quotidien ? Quelles pratiques de sécurité mettre en place ? Qu'est ce que ça implique, qu'est ce que ça créé en nous et à l'extérieur de nous ?

Voici 5 axes qui peuvent servir de pistes de réflexion. Cette liste n'est pas exhaustive.

- **NIVEAU DE SÉCURITÉ** : Quel niveau de sécurité mettre en place dans sa vie / ses activités? Dans quel contexte telle ou telle information est sensible et à protéger? Comment choisir un niveau de sécurité pertinent?

- **ORGANISATION COLLECTIVE** : Quels impacts la mise en place d'une culture de sécurité a sur une organisation collective? Dans quel moment / espace collectif la culture de sécurité se manifeste? Qu'est ce que ça complique dans une organisation collective? Qu'est ce que ça permet, facilite ?

- **LA CONFIANCE** : Qu'est ce que ça veut dire faire confiance à quelqu'un·e ? Comment s'articulent la confiance et la mise en place de pratiques de sécurité ? Comment nourrir des relations existantes au quotidien tout en maintenant de bonnes pratiques de sécurité ?

- **LES RENCONTRES** : Qu'est ce que ça provoque dans les rencontres ? Comment tisser des liens sincères et forts avec de nouvelles personnes sans divulguer d'informations sensibles, et sans amener l'autre à divulguer des infos sensibles?

- **LA TRANSMISSION** : Comment transmettre des infos / des expériences / des leçons en continuant à ne pas divulguer d'informations sensibles et en continuant à respecter le niveau de sécurité qu'on s'est donné (individuellement et/ou collectivement)?

PISTES DE RÉPONSES

Il n'y a pas de réponse toute faite à ces questions là. Les réponses sont à construire seul·e mais aussi et surtout collectivement, avec beaucoup de discussions, de temps et d'échanges. Voici en vrac quelques idées qui ont pu émerger lors de certaines formations autour de la culture de sécurité ou qu'on a piochées dans des brochures, des expériences, des discussions et qui amènent des éléments de réflexion qui nous paraissent pertinents.

C'est des idées qu'on a retranscrites telles quelles, sans forcément reformuler ce qui avait été dit/écrit, sans recontextualiser. Ça peut être bien à lire tout.e seul.e mais on se dit surtout que c'est utile si tu as fait une formation sur ces thèmes et que tu as envie de te souvenir d'idées qui auraient pu émerger lors de discussions ou bien dans un contexte de lecture collective, pour piocher des idées et discuter ensemble de comment ça nous parle, quels fils on en tire...

On n'est pas forcément d'accord avec tout ce qui suit et on vous invite surtout à faire attention à bien prendre en compte le contexte dans lequel vous vous trouvez avant d'adopter

des pratiques de sécurité. Et surtout: pensez vos modèles de menace, discutez collectivement dans les milieux dans lesquels vous vous organisez et avec les gens avec qui vous partagez du quotidien! On le redira jamais assez.

Blazes

Un blaze, c'est un pseudonyme, un nom qu'on utilise en général à la place de son prénom administratif ou de naissance.

☼ Avoir un blaze c'est un bon moyen de ne pas relier son identité civile à une action, un lieu, un groupe de personne...

☼ C'est très utile d'avoir un nom, une dénomination, un pseudo pour une personne. On peut pas juste se passer de prénoms, ou alors c'est vraiment très difficile!

☼ Pour demander son nom à quelqu'un·e on peut dire : comment je t'appelle? Comment tu veux que je t'appelle? La formulation de la question peut ouvrir la discussion, rendre plus léger le fait de ne pas donner certaines infos comme son prénom administratif.

☼ Changer de blaze selon les contextes ça peut aussi t'aider à segmenter tes activités, à te rappeler que dans tel contexte tu as tel blaze associé à telles pratiques de sécurité.

☼ Un pseudonyme est difficilement assez solide pour résister à une enquête poussée mais permet de mettre de la confusion et de faire perdre du temps aux enquêteurices : avoir plusieurs blazes associés à plusieurs contexte peut créer de la confusion chez les personnes qui essayeraient de comprendre ce qui se joue dans tel ou tel milieu, ville, réseau... (c'est à double tranchant car tes ennemis autant que tes allié·es peuvent avoir besoin de comprendre ce qui se passe).

☼ Changer de blaze permet aussi de jouer avec son identité et expérimenter différentes manières de se nommer.

☼ Dans un milieu où tout le monde se présente via un blaze (et a fortiori quand on capte direct que c'est un blaze et que c'est pas une identité civile (Loupiote, Cascade, Courgette, par exemple on capte direct que c'est pas ton prénom administratif, quoi...) ça peut vite devenir un marqueur d'appartenance au groupe d'avoir un blaze, en plus d'être lié à des enjeux de sécurité. Ça peut être un facteur d'exclusion pour quelqu'un·e qui n'a pas ces codes.
Ça peut être un bon levier pour commencer à intégrer des pratiques de sécurité, via l'envie d'entrer dans le groupe.

Circulation de l'information

☼ Lorsqu'on s'apprête à faire circuler une info, c'est cool de se poser la question de qui a besoin de cette information et de ne la donner qu'aux gens qui en ont besoin, au moment où ielles en ont besoin.
Avoir une info dont tu n'as pas besoin ça peut être inconfortable. Par exemple, si tu te fais interroger et qu'il faut que tu protèges une information, c'est beaucoup plus facile de le faire si tu n'as pas l'info en question.

☼ Ne pas donner une info à quelqu'un·e ne veut pas dire qu'on ne lui fait pas confiance. C'est peut être juste qu'iel n'a pas besoin d'avoir cette info.

☼ Voici plusieurs exemples de 'niveaux' de confidentialité répondant à des besoins différents[49] :

1) Seul·e·s celleux qui sont impliqué·e·s directement dans l'action ont vent de son existence.

2) Le groupe décide au cas par cas de dévoiler l'action à des personnes de confiance dont le soutien est nécessaire.

3) Le groupe peut inviter à participer à l'action des personnes qui pourraient refuser — il en résulte que des personnes extérieures peuvent être au courant de l'action, tout en étant censées tenir leur langue.

4) Aucune liste précise de personnes invitées n'est dressée ; les participant·e·s peuvent inviter d'autres personnes et les encourager à faire de même, tout en insistant sur la nécessité de garder l'information dans des sphères dignes de confiance pour en conserver le secret.

5) Des « rumeurs » de l'action peuvent être largement répandues au sein de la communauté, mais l'identité des personnes centrales pour son organisation doit rester secrète.

6) L'action est largement annoncée, tout en conservant un minimum de discrétion, afin que les autorités les plus somnolentes n'en aient pas vent.

7) L'action est annoncée publiquement par tous les moyens possibles.

☼ C'est difficile de savoir si une info est sensible ou pas avant qu'elle ait été utilisée pour la répression.

☼ Une absence flagrante d'info (aucun paiement par carte bleue, pas de présence sur les photos, etc.) EST une information, qui peut se révéler être sensible (par contraste).

☼ Parfois donner des informations sensibles peut être nécessaire à une personne ou à un groupe afin de comprendre un contexte particulier. C'est dur de faire le tri dans ce qui est nécessaire ou pas...

Qu'est ce que ça veut dire 'faire confiance'?

☼ Il y a des sphères de confiance différentes, par exemple : je compte sur cette personne pour organiser un projet collectif, mais pas pour m'aider pour mon prochain déménagement.
On associe souvent confiance et confidence. Peut être que la confidence ce n'est qu'une des sphères de la confiance.

☼ pourquoi je fais confiance à cette personne ?

- j'ai des infos perso/sensibles/intimes sur elle ?
- elle a des infos perso/sensibles/intimes sur moi ?
- on a vécu des moments (forts, nombreux) ensemble ?
- on a participé ensemble à des projets collectifs ?
- on a réussi à dépasser des obstacles ensemble ?
- on a des convictions communes ?
- je sais qu'elle est sensibilisée à la culture de sécurité ?
- on a des codes communs ?
- je me sens bien avec elle, le feeling passe bien ?

☼ C'est déstabilisant de changer la manière dont on reçoit/donne la confiance. C'est tout un apprentissage. Il faut prendre soin des gens pour contrebalancer.

---

49 https://crimethinc.com/2004/11/01/cultures-de-la-securite *Cultures de la sécurité*, 2004

☼ On a beaucoup intégré des différences de valeur/préciosité entre différentes infos (différence de préciosité et donc de curiosité envers un nom d'enfance versus un blaze inventé il y a deux semaines).
☼ On doit changer de stratégie pour faire confiance, on ne peut pas juste enlever des manières de faire confiance et ne rien réinventer derrière.

L'honnêteté

☼ Comment ne pas se sentir coupable de 'mentir'? Comment continuer à se sentir honnête (notamment auprès de ses proches) quand on ne partage pas tout? Quand on ne partage pas des évènements forts, marquants de notre vie? Comment partager des évènements forts, marquants sans divulguer d'informations sensibles?

☼ Entre gens qui partagent du quotidien, ça semble préférable de ne pas donner toutes les informations (et d'accepter de ne pas avoir toutes les informations, que certaines questions restent sans réponses) plutôt que de devoir mentir (sur où on va, ce qu'on a fait...).

Mettre en place des pratiques de sécurité

☼ Mettre en place des pratiques de sécurité dans sa vie ou ses activités, c'est beaucoup plus facile et efficace si les gens autour de soi le font aussi : on peut s'entraider, décider ensemble de ce qui est pertinent, partager nos bourdes.

☼ Faire des erreurs c'est NORMAL! Si tu t'es planté·e, reste pas tout·e seul·e avec ça, parles-en et prenez ça en charge collectivement.

☼ On ne change pas seul·e. C'est difficile de faire face à une asymétrie de changement avec son entourage.

☼ C'est bien de s'entraîner à mettre en place des pratiques de sécurité avant d'en avoir vraiment besoin, pour pouvoir faire des erreurs sans (trop) stresser.

☼ Le stop, les covoiturages, c'est des bons endroits pour s'entraîner à changer ces manières de communiquer avant d'en avoir vraiment besoin.

Avoir des sources

☼ C'est très utile de se renseigner sur les risques, les affaires similaires, les techniques de surveillance/répression utilisées dans ce genre de contexte... Ça permet de rationaliser le niveau de sécurité qu'on met en place, de prendre des décisions en se basant sur des « faits », des données plutôt que sur des rumeurs, des projections infondées, des peurs... Il y a des gens qui fantasment un état et une police omnipotentes. Il y a des gens qui ne captent pas à quel point la répression et le fichage c'est courant.

⚠ C'est quand même aussi utile de prendre en compte le ressenti des personnes concernées lorsqu'on met en place des pratiques de sécurité: améliorer sa sécurité c'est bien, améliorer sa sécurité ET se sentir plus en sécurité c'est beaucoup mieux. Et se sentir en sécurité alors qu'on ne l'est pas, c'est dangereux.

☼ Nécessité d'une connaissance solide des risques pour accepter le coût de mise en place de solutions adéquates.

☼ Problème chiant: les outils d'attaque et de protection, ça évolue vite. Ça demande de se tenir au courant, d'y passer du temps.

Les pratiques de sécurité et le groupe

☼ Comment faire quand dans un groupe les différentes personnes ne sont pas d'accord sur le niveau de sécurité à mettre en place? Est ce qu'on adopte le niveau de sécurité de la personne qui a le plus grand degré d'exigence? Elle a peut être ce niveau d'exigence parce que ses activités dans ce groupe peuvent être mises en lien avec d'autres parties de sa vie et qu'elle ne peut pas se permettre que ce lien soit fait par les personnes qui pourraient la surveiller.

☼ Comment réagir lorsque le groupe dans lequel tu t'organises ne met pas en place un niveau de sécurité suffisant pour toi ? Est-ce que ça peut t'amener à quitter le groupe ?

☼ Comment réagir quand une personne du groupe ne respecte pas le niveau de sécurité qui a été décidé collectivement? Il faut donner la possibilité aux personnes de respecter le niveau de sécurité qu'on se donne (par la formation, le partage de connaissances, compétences, le soutien dans l'apprentissage...). Est-ce que c'est envisageable de pratiquer l'exclusion?

Impacts psychologiques

☼ Parfois y a besoin d'exprimer ce qu'on fait parce que ça nous a touché, que c'est dur à vivre.

☼ Avoir différentes identités dans différents groupes, ne pas donner les mêmes infos à tout le monde, devoir se rappeler quelles infos on a données à qui pour ne pas faire de gaffe... ça peut être usant.

☼ Les psys : Ça peut être quelqu'un·e auprès de qui je vide mon sac, avec qui je suis entièrement transparent·e

Est ce que ça suffit (même s'il n'y a pas de lien affectif)?

☼ Si on est un peu stressé·e par le contact entre flics et psychologues, c'est potentiellement dur de faire confiance à un·e psy, sachant qu'en plus la loi n'est pas très claire sur si iels sont soumis·es au secret professionnel ou non. Il existe un code déontologique (non contraignant) qui leur interdit de divulguer des informations personnelles sur leurs patient·es[50]. Et récemment le Ministère de la santé et de la prévention s'est positionné en disant que les psychologues étaient soumis·es tout comme les médecins au secret professionnel[51]. Seulement, le secret professionnel ne nous protège pas de tout[52], et peut être brisé sous certaines conditions [53].

☼ C'est cool si on se fait passer les listes de bons psys[54]!

☼ Quand on est en contact avec des gens qui n'ont pas du tout les mêmes codes que nous, qui ne partagent pas la même culture de sécurité (ex: la famille, au travail), ça peut être difficile.

---

50 https://www.codededeontologiedespsychologues.fr/IMG/pdf/Code_deontologie_psychologue_9-09-2021.pdf Voir secret professionnel, p3

51 https://www.senat.fr/questions/base/2022/qSEQ220701818.html

52 Site avec moult lectures sur les questions de psychiatrie https://www.zinzinzine.net/

53 Cadre légal de la violation du secret professionnel : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417952/2023-06-03/

54 https://psysafeinclusifs.wixsite.com/psysafe/get_involved *Psys Situé·e·s prenant en compte les oppressions systémiques*, Psys Safes Inclusifs (liste de psys chouettes selon les villes)

Choisir un niveau pertinent de sécurité

☼ Est ce qu'il vaut mieux un niveau de sécurité moyen bien respecté ou un niveau de sécurité élevé mal respecté ?

☼ Est ce que certaines pratiques sont efficaces même si elles ne sont pas très bien respectées ? Par exemple les blazes, qui peuvent amener de la confusion (et peut être encore plus de confusion s'il y a des erreurs qui ne sont pas visibilisées comme telles).

☼ Trop de sécurité tue la sécurité ?

☼ Pour les personnes n'ayant pas d'activités militantes mais qui côtoient des personnes en ayant : quelles exigences de sécu on se donne ? Dans l'équilibre entre ne pas trop attirer l'attention avec trop de protection mais sans mettre en danger son entourage.

Street-cred et besoin de reconnaissance

La *street-cred*, c'est quand tu racontes des actions militantes, des histoires qui te sont arrivées pour te faire remarquer, avoir de la crédibilité, impressionner les autres, montrer que toi (aussi) tu es un·e (vrai·e) militant·e.

☼ Y a de l'égo quand on raconte les choses qu'on fait, c'est important de travailler l'humilité mais on a aussi besoin de reconnaissance pour continuer à faire ce qu'on fait, à avoir de l'enthousiasme et de l'énergie. Comment on se donne l'envie de s'engager ?

☼ Se raconter des histoires qu'on connaît, c'est une bonne manière de faire groupe.

Culture de sécurité et considérations stratégiques

☼ Différentes stratégies de lutte : beaucoup de structures militantes basent leurs luttes plutôt sur l'ouverture, l'implication du grand nombre. Quelle place une personne certainement fichée peut prendre dans une telle structure ?

☼ Comment faire s'articuler les différentes pratiques de sécu des différents milieux militants ?

Interactions et rencontres

☼ Quel niveau de dévoilement on met spontanément au cœur de nos conversations / relations ? Les enjeux habituels qui se jouent autour de nos manières de nous rencontrer, d'échanger impliquent souvent un haut niveau de dévoilement tout en étant assez superficiels.

☼ Les sujets de discussion habituels à questionner: t'es d'où ? où t'as grandi ? On a des potes commun·es ? projets ? politisation ? habitudes ?

☼ Il faut trouver d'autres moyens de se présenter que l'historique, le CV (j'ai fais telles études, je viens de telle ville, je bosse là...). Pour se rencontrer sans se mettre en danger (ex: qu'est ce que j'aime faire ? C'est quoi les trucs du corps humain trop chelous qu'on trouve dégueu ? Quelle musique j'écoute ? La dernière BD tellement stylée qu'on a pleuré ? ...).

☼ Partager son vécu ça peut être vecteur de lien si on partage du vécu commun.

La segmentation (ou compartimentation)

☼ Segmenter ses activités c'est avoir différentes pratiques de sécurité selon les milieux. Différents blazes, différents niveaux de confiance... Mais c'est pas toujours facile de segmenter sa vie, parfois c'est poreux. Ça demande pas mal de compétences pour gérer ça.

PISTES DE RÉFLEXIONS À L'USAGE DES COLLECTIFS

Voici quelques questions et pistes de réponses plus tournées vers l'organisation collective, qui nous semblent pertinentes d'avoir à l'esprit quand, en tant que groupe, vous vous emparez de la question de la sécurité et tentez d'intégrer ces enjeux à votre fonctionnement interne. Nous compilons ici des pistes de réflexions en nous basant sur des lectures et sur des retours de formations qui ont été données autour de la culture de sécurité.

Comme pour la partie précédente, ce sont des idées qui n'ont pas forcément été reformulées, avec lesquelles on est pas toujours complètement en accord et qui peuvent servir à la réflexion, qu'elle soit individuelle ou collective. Elles peuvent également être utile dans une dynamique d'élaboration d'un modèle de menace.

Circulation des infos en interne

☼ Est ce qu'on prend des notes durant les réunions ? Sur un ordinateur ? Sur une feuille papier ?

☼ Quelles infos sont mises dans ces notes et quelles infos n'y sont pas ? Comment savoir quelles infos mettre ou ne pas mettre pour ne pas laisser derrière les personnes qui auraient accès seulement au compte-rendu ? Comment ces notes sont-elles conservées ?

☼ Comment on détermine collectivement le niveau de sensibilité d'une information ?

☼ Comment les notes ou les comptes-rendus sont-elles partagées, par exemple aux personnes qui ne sont pas présentes aux réunions ?

☼ Quels outils on utilise pour communiquer (mails ? textos ? oral ?) ?

Répression

☼ Qu'est ce qu'on fait dans notre groupe qui pourrait nous exposer à de la répression ? Est ce qu'on a des exemples de groupes similaires ? Quel genre de répression ont-ils subi ou subissent-ils ?

☼ Comment désamorcer collectivement les propos qui freinent la mise en place de pratiques de sécurité/les personnes qui dénigrent ce besoin ? (à ce sujet, voir dans les **Annexes** *Les remarques qu'on entend souvent sur la mise en place de pratiques de sécurité et comment y répondre*)

☼ Est-ce qu'on est ou on voudrait être en lien avec des groupes qui s'exposent plus à la répression que nous ? Si oui, comment faire en sorte de ne pas, au travers de notre lien ou de nos échanges, divulguer des informations sensibles pour ce collectif ? Comment faire en sorte que ce lien ne nous expose pas à une répression inutile/évitable ?

Accueil de nouvelles personnes

☼ Comment on accueille des nouvelles personnes en conservant de bonnes pratiques de sécurité ?

☼ Comment on fait en sorte que de nouvelles personnes se sentent les bienvenues, intégrées au groupe même si, par exemple, on ne leur dévoile pas tout ce qui se passe au sein du groupe ?

☼ Comment on fait en sorte que les nouvelles personnes adoptent les pratiques de sécurité qui ont été définies comme pertinentes par le groupe ? Comment on transmet les pratiques en place et/ou on s'adapte aux pratiques de la nouvelle personne ?

☼ Comment on fait en sorte de sensibiliser sur ces sujets sans faire peur ?

☼ Comment on se protège d'éventuelles taupes sans faire fuir / exclure d'éventuel.les allié.es ? Comment gérer lorsqu'on est pas sûr·e d'une personne et/ou lorsqu'on s'est fait infiltrer ? Comment gérer sans faire exploser le groupe, sans exclure une personne par erreur[55] ?

Diffusion des informations et lien avec le public et les institutions

☼ Notre groupe est-il reconnaissable publiquement ? A-t-il une existence, juridique ou non, qui le rend identifiable ?

☼ Est-ce que des personnes du collectif sont identifiables (photo, identité civile...) et identifiables comme faisant partie du groupe (photo dans des évènements, signe distinctif (tee-shirt, badge...)) ?

☼ Si des actions répréhensibles sont portées par le groupe, qui s'expose à de la répression (la structure ? des individu·es identifié·es comme faisant partie du groupe ?) ?

☼ Est ce que le groupe a besoin de communiquer des informations publiquement ? Si oui, comment ? Via une adresse mail collective ? Qui s'y connecte ? Avec quel appareil ?

☼ Comment trouver l'équilibre entre le soutien à des groupes/personnes alliées dont les activités sont légalement répréhensibles et des liens éventuels avec des institutions (subventions, partenariats...) ?

Segmentation

☼ Est ce que notre groupe a plusieurs activités, dont certaines exposent à peu/pas de répression et d'autres à plus de répression ? Est-il pertinent d'avoir différents niveaux de sécurité pour nos différentes activités ?

☼ Comment réussir à jongler entre différents niveaux de sécurité au sein d'un même groupe ?

55 https://www.infiltration.fail/ *The story of how one activist group kept ourselves safe and strong in the face of movement infiltration*, Damage Control, 2015

Tentative de protocole

Une possibilité intéressante pour se lancer dans la réflexion, ce serait :

1. Poser un cadre aux actions du groupe, sans nécessairement rentrer dans le détail : Quel type d'actions ? Quelle taille de groupe ?
2. Identifier les menaces qui peuvent peser sur l'organisation/les activités. Cette étape se fait via de la recherche d'informations : quelle répression a pesé sur des groupes similaires par le passé par exemple ?
3. Réfléchir à la façon dont on répond à ces menaces : Utiliser des blazes ? Ne jamais amener son téléphone en réunion ? Utiliser des outils de communication sécurisés ? Certaines questions peuvent demander à nouveau des recherches pour être au clair avec les enjeux techniques.
4. Prendre des décisions communes et explicites.

Il est probable que les différentes activités d'un groupe ne demandent pas toutes le même niveau d'attention à la sécurité. Il faudra sans doute répéter ces recherches et discussions pour ces différentes activités, mais aussi considérer la façon dont elles se combinent.

Conclusion

Ces idées peuvent aider à la réflexion, donner des pistes pour voir un peu l'étendue des sujets que l'on peut creuser lorsqu'on s'attaque au thème de la culture de sécurité. Ces sujets sont très vastes, et en plus des discussions possibles entre ami·es, camarades de lutte etc, il y a pas mal de documentation, notamment sous forme de brochures, qui existe pour aller plus loin[56] [57].

56 https://infokiosques.net/prison_justice_repression Infokiosques.net, rubrique Prison, Justice, Répression

57 http://aka3xvhiygnchpsbrilphkzbdxtvr6j6pc7hluf6mf2ddruttsikswad.onion/fr/ Centre de documentation sur la contre-surveillance

Comprendre les ordinateurs, internet et tout ce merdier

Introduction

L'informatique est un outil de communication très utilisé dans beaucoup de réseaux militants. Y laisser des traces est facile et il est difficile de comprendre et de maîtriser ces traces sans avoir un minimum étudié la question.

Dans cette partie nous vous proposons d'essayer de mieux comprendre comment fonctionnent une partie des outils numériques que nous utilisons (ordinateurs, internet, mails...) afin de pouvoir identifier quelles sont les traces qu'on y laisse et qui y a accès.

Ordinateur

Matériel

Un ordinateur est composé de trois éléments essentiels (voir schéma 1):

Le processeur : fait les calculs, c'est à dire fait toutes les opérations qui permettent à l'ordinateur de fonctionner.

La mémoire vive : stockage de données. C'est une sauvegarde temporaire car elle se vide entièrement peu de temps après avoir éteint l'ordinateur[58]. L'accès à cette mémoire est très rapide.

Le disque dur : stockage de données. C'est une sauvegarde pérenne (les données restent sauvegardées même quand on éteint l'ordinateur) mais dont l'accès est plus lent que la mémoire vivre. Une clé USB a le même rôle qu'un disque dur: c'est un espace de stockage pérenne mais lent.

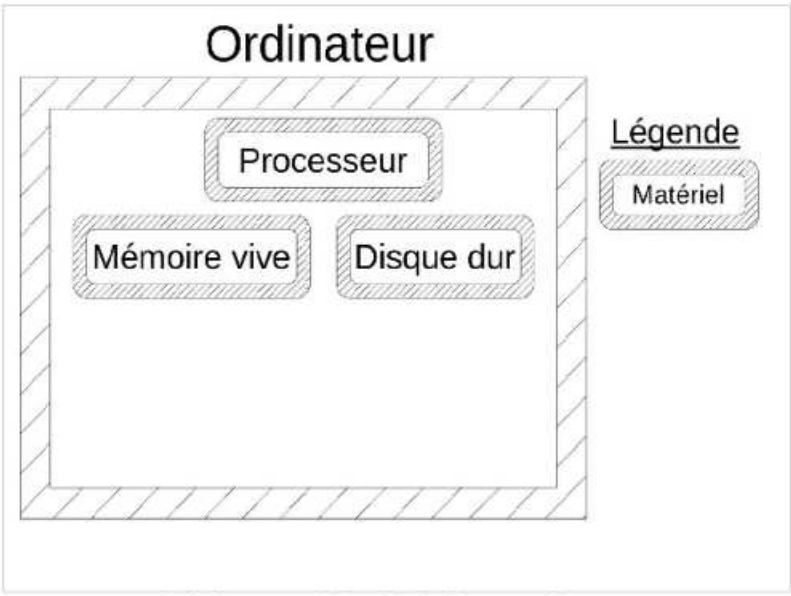


Schéma 1 : Matériel d'un ordinateur

58 C'est pas complètement immédiat, et ça peut mener à de possibles (et rares) attaques : https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9marrage_%C3%A0_froid

Un ordinateur peut également intégrer des périphériques, qu'on branche sur l'ordinateur pour interagir avec lui ou pour qu'il interagisse avec d'autres ordinateurs. Ce sont les interfaces ou intermédiaires entre quelqu'un·e et un ordinateur ou entre un ordinateur et un autre ordinateur. Le clavier, la souris, l'écran, la carte réseau sont des périphériques assez classiques.

Informations

Un ordinateur c'est donc une machine, dont on a vu les composants essentiels, mais ce sont aussi des informations qui sont enregistrées et/ou qui circulent dans les différents composants de cette machine (voir schéma 2).

Quelles types d'information trouve-t-on dans un ordinateur ?

Les informations présentent dans un ordinateur se présentent à nous sous la forme de **fichiers**. On trouve des fichiers qui sont assez familiers: des textes, des photos, des films... On trouve également des **logiciels**, ce sont des fichiers dans lesquels il y a des instructions pour l'ordinateur.

Par exemple, un logiciel de traitement de texte est un fichier dans lequel on trouve l'instruction suivante: lorsque l'utilisateurice sélectionne une portion de texte et clique sur l'icône *I*, le texte sélectionné se met en italique.

Un autre exemple c'est le **système d'exploitation**, qui est un logiciel qui s'occupe entre autre de faire l'interface entre les composants matériels et les autres logiciels présents sur l'ordinateur.

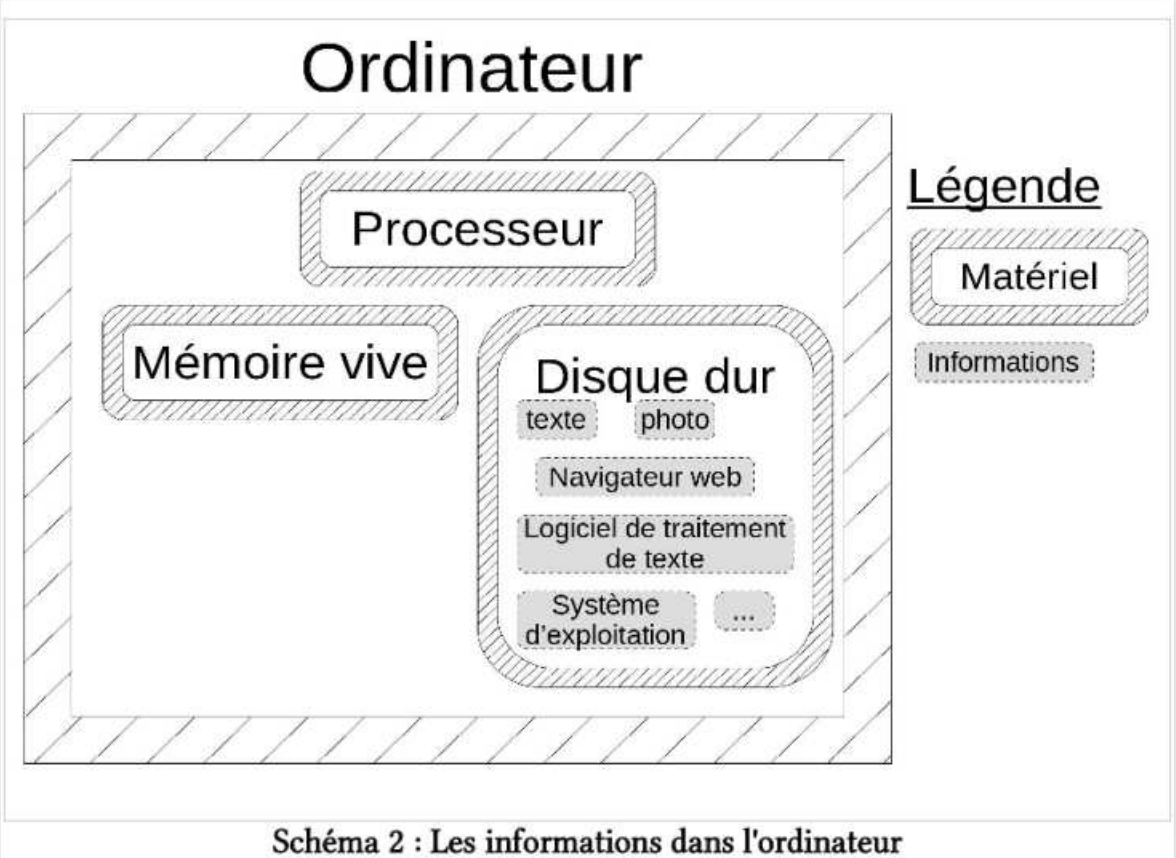


Schéma 2 : Les informations dans l'ordinateur

Où se situent ces informations dans un ordinateur?

Les informations présentes sur un ordinateur sont enregistrées de manière pérenne sur le **disque dur** mais peuvent aussi être enregistrées de manière transitoire sur la **mémoire vive** (voir schéma 3).

Prenons l'exemple d'un **fichier** texte. Il est rangé dans le **disque dur**. Lorsque j'ouvre ce fichier texte pour le modifier, une copie est enregistrée dans la **mémoire vive** pour permettre des modifications quasi-instantanées. On voit dans cet exemple la différence de vitesse entre le disque dur (mémoire lente) et la mémoire vive (mémoire rapide): mon fichier texte met souvent quelques secondes à s'ouvrir, c'est qu'il faut aller le chercher dans le disque dur. Par contre, une fois ouvert (une fois qu'une copie a été faite dans la mémoire vive), les modifications que je fais sont ultra-rapides. Si j'enregistre mon fichier texte, une copie de la version modifiée (présente dans la mémoire vive) vient remplacer l'ancienne version sur le disque dur.

Il en est de même pour tous les fichiers (y compris les logiciels!): lorsqu'ils sont ouverts, ils sont en partie copiés dans la mémoire vive puis, une fois fermés, ils sont rangés dans le disque dur.
Lorsqu'elle n'est pas alimentée par de l'électricité, la mémoire vive se vide entièrement.

Les fichiers sont donc rangés dans le disque dur. Pour permettre aux différents logiciels (et notamment au système d'exploitation) de retrouver les fichiers dans le disque dur, celui-ci possède un **index**, qui fonctionne comme une sorte de table des matières qui indique où sont rangés les fichiers.

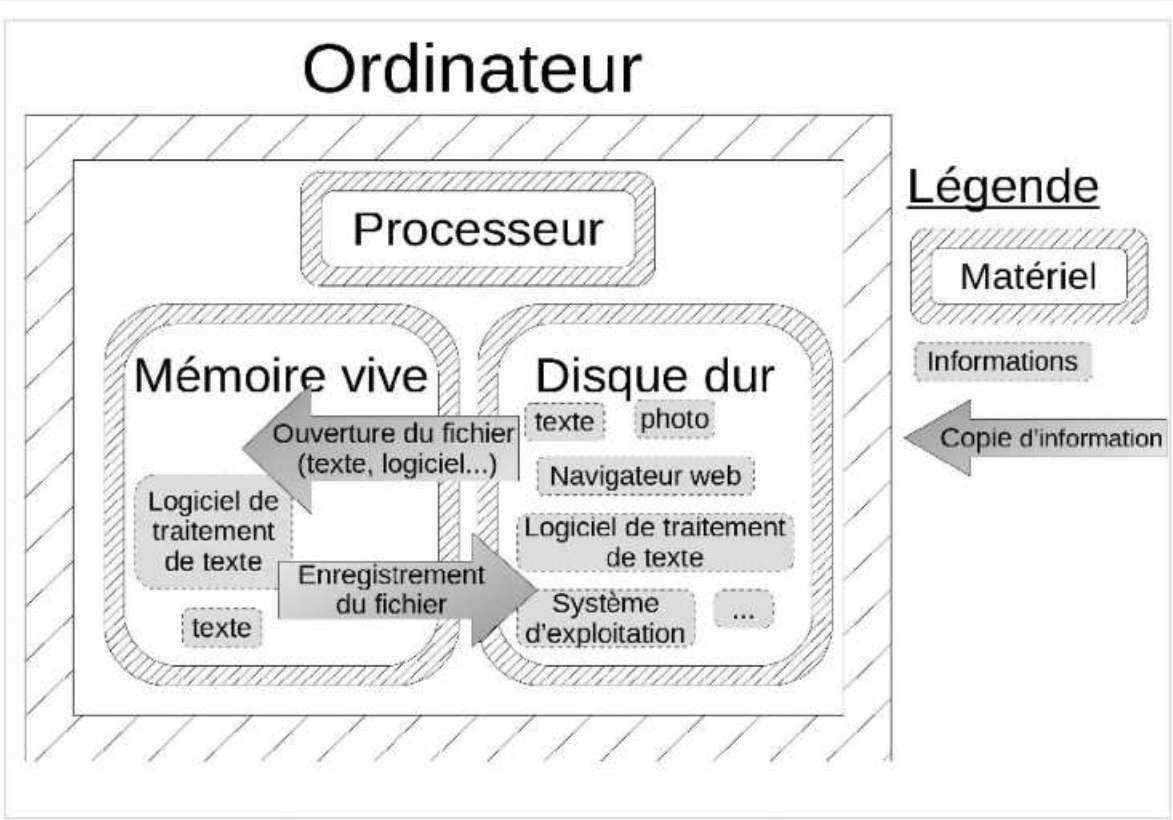


Schéma 3 : Comment circulent les informations

Protéger les informations qui sont sur mon disque dur, ma clé usb

Si on se replonge dans ce qui nous intéresse, c'est à dire la mise en place de pratiques de sécurité, on peut imaginer par exemple un texte sur lequel il y a des informations sensibles. On va se demander comment est ce que quelqu'un·e pourrait avoir accès à ce texte et étudier ces différents scénarios pour comprendre comment protéger ce texte.

↣ Scénario 1 : Accès physique à l'ordinateur

Quelqu'un·e récupère notre ordi ou notre disque dur (par exemple lors d'une perquisition) et va essayer d'avoir accès aux informations qui sont enregistrées dessus.

> ⚠ Un mot de passe lié à votre système d'exploitation, qui servirait à ouvrir votre session d'utilisation, ne protège pas vos données. Il est possible de contourner ce mot de passe, par exemple en prenant le disque dur de votre ordinateur et en le branchant sur un autre ordinateur.

Il y a plusieurs manières de protéger nos données dans cette situation :

☛ Suppression et écrasement d'un fichier

La manière la plus simple d'empêcher qu'un fichier soit lu par quelqu'un·e d'autre que vous est de le supprimer. Il y a plusieurs niveaux de suppression d'un fichier :

😶 placer le fichier dans la corbeille. Dans ce cas le fichier est encore facilement accessible, il est juste déplacé dans un dossier qui s'appelle Corbeille.

😮 supprimer le fichier, vider la corbeille. Ce qui se passe dans ce cas c'est que le système d'exploitation supprime dans l'index la ligne correspondant au fichier. Le fichier n'est plus répertorié dans l'index mais il est encore présent dans le disque dur. La place qu'il occupe n'étant pas répertoriée comme occupée dans l'index, elle va à terme être utilisée pour enregistrer d'autres fichiers qui vont être réécrits par dessus le fichier d'origine. À ce moment là le fichier n'est plus lisible mais cela peut prendre des mois voire des années et ça reste incertain. En attendant, le fichier reste lisible pour un logiciel qui parcourrait directement le disque dur, sans passer par l'index.

😵 écraser un fichier. Certains systèmes d'exploitation offrent la possibilité d'écraser un fichier. Dans ce cas la ligne correspondante dans l'index est supprimée et le système d'exploitation réécrit plusieurs fois des données aléatoires à l'endroit où le fichier était enregistré. De cette manière il n'est plus lisible par quiconque essayerait d'y accéder.

> ⚠ Cette technique ne fonctionne pas de manière sûre, par exemple si le fichier a été modifié et enregistré plusieurs fois (soit par le logiciel soit par toi) ou sur les disques durs SSD ou les clés USB (en raison de la manière dont les enregistrement se passent sur ce type de mémoire).
>
> Dans tous les cas, la seule manière pour être 100% sûr·e d'effacer toutes traces d'un fichier compromettant est de procéder à l'écrasement de tout l'espace disque disponible, c'est à dire tous les espaces de mémoire qui ne sont pas répertoriés dans l'index.

☛ Chiffrement d'un fichier

Une autre manière de protéger un fichier d'une personne ayant accès à votre disque dur est de chiffrer ce fichier.

Chiffrer un fichier c'est comme coder un message. Lorsqu'un message est codé, il ne signifie rien pour la personne qui n'a pas le code, qui ne sait pas comment déchiffrer le message et le rendre à nouveau lisible. Lorsqu'on chiffre un fichier, on le rend illisible et protégé par un mot de passe (par exemple) qui permet de rendre le fichier à nouveau lisible.

Pour qu'un fichier soit bien protégé, il faut que le mot de passe soit efficace: qu'il soit long, intègre des caractères spéciaux, etc. (pour plus de détails, voir la section *Mots de passe).*

Légalement, la justice peut, sous certaines conditions, demander de donner ce mot de passe. Ces conditions sont décrites dans les annexes, dans la section *Quelques éléments d'anti-répression*, avec des précisions légales sur les enjeux autour de la divulgation de mots de passe.

Certains logiciels permettent de chiffrer un fichier mais c'est aussi possible de chiffrer tout un dossier ou même tout un disque dur. Des outils de chiffrement sont détaillés dans la partie *S'outiller pour avoir une utilisation sécurisée des outils numériques.*

↣ Scénario 2 : Accès aux données via un logiciel

Des fichiers peuvent aussi être récupérés à distance, sans que la personne voulant y accéder ait directement accès au matériel ou après qu'elle y ait eu accès. La plupart du temps cette surveillance à distance se fait via des logiciels ou du matériel installés sur l'ordinateur.

⚯ Un logiciel de surveillance

Il y a plusieurs manières pour une personne d'installer un logiciel de surveillance sur un ordinateur :

▸ si la personne a eu accès à l'ordinateur (ex : si l'ordinateur a été saisi puis rendu à son/sa propriétaire).

▸ via une clé usb qui peut être programmée pour télécharger un logiciel sur tous les ordinateurs sur lesquels elle va être branchée.

▸ via une faille de sécurité dans un logiciel : il existe des failles de sécurité dans certains logiciels qui permettent par exemple de cacher un logiciel de surveillance dans un fichier. Ce logiciel s'installe sur l'ordinateur par exemple au moment du téléchargement du fichier depuis internet. Les mises à jour des logiciels servent en grande partie à réparer ces failles de sécurité, d'où l'importance de faire des mises à jour régulièrement.

Ces logiciels de surveillance vont prendre des infos sur un ordinateur et les font sortir par la carte réseau de cet ordinateur pour les envoyer vers d'autres ordinateurs.

⚯ Un logiciel de « surveillance »?

Dans le paragraphe précédent on imagine qu'un nouveau logiciel est installé sur un ordinateur dans le but de récupérer des informations sur cet ordinateur. Mais le fait est que beaucoup de logiciels que nous utilisons au quotidien servent à récupérer des informations sur notre ordinateur et à les envoyer vers d'autres ordinateurs. Sont-ils pour autant des logiciels de surveillance?

▸ Certains de ces logiciels font effectivement sortir des informations de l'ordinateur, mais de manière transparente et dans l'intérêt des personnes qui utilisent ces logiciels.

> Par exemple, un gestionnaire de boîte mail qui va envoyer des mails vers d'autres ordinateurs.

▸ Certains le font de manière moins transparente, mais encore dans l'intérêt de l'utilisatriceur.

> Par exemple, les systèmes d'exploitation qui demandent les mise à jour des logiciels utilisés.

▸ D'autres logiciels font sortir des informations de l'ordinateur en le cachant et pour l'intérêt de personnes tierces (créateurices du logiciel en question, entreprises...).

> Par exemple, certains navigateurs **web** vendent les informations de connexion de leur utilisateurices (quels site web sont visités, à quelles fréquences, à quels moment de la journée?)

Si ce sont en général des entreprises qui récoltent ces données, la police et la justice peuvent également y accéder via des requêtes judiciaires. Par exemple en 2021 la France à envoyé environ 16 000 requêtes à Google, qui a répondu positivement dans plus de 80% des cas[62].

Parmi ces logiciels, certains peuvent récupérer des infos qui pourrait être demandées puis utilisées par la police mais au-delà de ce risque, on peut avoir envie de lutter juste contre le fait que nos informations soient récupérées sans notre consentement éclairé par des personnes tierces par exemple une grosse entreprise.

On sort un peu des questions de répression étatique, mais comme dit précédemment les Google, Apple, Facebook et compagnie font leur beurre sur l'exploitation des données informatiques. Leur fonctionnement c'est de réaliser un fichage généralisé qui leur permet de comprendre les habitudes et mécaniques de consommation de chacun·e, et par là même de supposément[55] augmenter l'efficacité de leurs publicités.

Un truc spécifique dans notre rapport à ces entreprises : certaines proposent des outils numériques qu'on peut avoir envie d'utiliser (WhatsApp pour Facebook par exemple, ou Windows pour Microsoft). Utiliser leurs outils c'est leur donner du pouvoir sur nous (surveillance, fichage). D'autant plus qu'on peut rarement savoir exactement ce que fait tel ou tel logiciel. Est-ce que Google lit mes mails Gmail ? Est-ce que Apple surveille la manière dont je me sers de mon téléphone ? Est-ce que Google Chrome envoie des informations sur ma navigation sur le web à Google ? Et bien plutôt oui[56 57], mais on a pas moyen de savoir réellement ce qu'il se passe.

59 https://ploum.net/lorsqueclatera-la-bulle-publicitaire/ *Lorsqu'éclatera la bulle publicitaire*, Ploum, 2022

60 https://www.theregister.com/2022/11/14/apple_data_collection_lawsuit/ *Apple sued for collecting user data despite opt-outs*, 2022 (article en anglais sur Apple qui collecte des données même quand les utilisateurices ont refusé de les partager avec les applications)

61 https://contrachrome.com/ContraChrome_fr.pdf, *Contrachrome*, 2022, (une chouette BD sur Chrome écrite par un repenti de Google)

62 Un rapport de Google sur l'ensemble des demandes judiciaires et diplomatiques que l'entreprise reçoit dans le monde *https://transparencyreport.google.com/user-data/overview*

Tout ça pour dire : on peut aussi vouloir renforcer ses pratiques de sécurité pour :
★ Se donner un peu d'intimité dans cet univers de surveillance constante, sans nécessairement abandonner l'usage de l'ordinateur.
★ Résister comme on peut à l'extension du capitalisme de surveillance[63]
(surveiller ⟹ comprendre les gens ⟹ les influencer de différentes façon, notamment leur vendre des trucs).

Que se soit pour se protéger de la répression ou juste se protéger du capitalisme de surveillance, ça pose la question de la confiance qu'on donne à un logiciel[64]. Qui l'a écrit, dans quel but, est-ce que je peux avoir accès au mécanisme en entier ?

Nous détaillerons plus loin des critères pour aider à choisir ses logiciels, mais le fait que ce soit un logiciel libre offre déjà une certaine garantie. En effet, le logiciel libre est une façon de faire des logiciels une propriété commune en permettant à tout le monde de les utiliser, de les modifier, de les diffuser. En très gros ça consiste à profiter de son droit d'auteur pour, au moment de publier un logiciel, dire (et écrire): « Ce logiciel ne m'appartient pas, c'est une propriété collective, faites-en ce que vous voulez »[65] [66]. Pour que cela soit possible, un logiciel libre est toujours transparent sur la façon dont il fonctionne (pour des personnes compétentes). Ceci nous donne certaines garanties sur le fait qu'il n'est pas un logiciel espion sans le dire.

↣ Scénario 3 : Accès aux données via du matériel de surveillance

Plutôt que d'installer un logiciel directement sur un ordinateur (c'est à dire dans son disque dur), il est aussi possible d'installer du matériel de surveillance qui se charge de récupérer des informations et de les envoyer à d'autres ordinateurs. Contrairement aux logiciels, pour installer du matériel il faut avoir accès à l'ordinateur. Mais ça peut être le cas, par exemple suite à une perquisition ou bien dans des salles informatiques de lieux collectifs. On ne détaille pas les différentes menaces de ce type mais elles existent[67].

LIEU DE VIE

Maintenant qu'on a vu comment fonctionne un ordinateur dans les grandes lignes on peut dézoomer et regarder ce qui se passe à l'échelle d'un lieu de vie. On utilise plein d'autres machine que notre ordinateur: notre téléphone, une imprimante, une box internet... Tous ces appareils sont en réalité des ordinateurs !

Ils sont composés d'un processeur, d'une mémoire vive et d'un disque dur sur lequel sont enregistrés des fichiers, notamment des logiciels qui permettent le fonctionnement de ces appareils mais aussi des informations sur la manière dont sont utilisés ces appareils (par exemple une imprimante peut garder en mémoire que tel ordinateur a demandé l'impression de tel fichier).

Vigilance donc dans l'utilisation de ces appareils !

63 https://fr.wikipedia.org/wiki/%C3%89conomie_de_la_surveillance#Capitalisme_de_surveillance, *Capitalisme de surveillance*, Wikipédia
64 Voir les histoire avec Apple ou Chrome citées précédemment, miam miam !
65 https://fr.wikipedia.org/wiki/Logiciel_libre, *Logiciel libre*, Wikipédia
66 https://www.gnu.org/philosophy/free-sw.fr.html, *Qu'est-ce que le logiciel libre ?*, gnu.org
67 https://earsandeyes.noblogs.org/fr/, (un site cool qui répertorie les différents dispositifs de surveillance, les endroits où on a déjà retrouvé des dispositifs de surveillance, etc.)

INTERNET

Pour cette partie nous vous conseillons de vous référer aux schémas qui aident beaucoup à la compréhension des textes.

Internet c'est un système (des câbles, des ordis, des protocoles) qui connecte des ordinateurs entre eux.

Pour que la communication soit possible entre les ordinateurs il y a des accords qui ont été trouvés sur des manières de communiquer (ex: comment ils s'interpellent, dans quel ordre ils se donnent les infos...). C'est ces manières de communiquer qu'on appelle des **protocoles**.

On appelle certains ordinateurs qui composent internet des **serveurs**. Ce terme désigne plus le rôle qu'un ordinateur peut avoir qu'un type de machine particulier. On appelle serveur un ordinateur (processeur + mémoire vive + disque dur) qui rend disponible via internet (et dans l'immense majorité des cas de manière continue) tout ou une partie des **fichiers** qui sont sur son disque dur. Dans les faits, les ordinateurs qui tiennent ce genre de rôle au sein d'internet sont des ordinateurs qui sont spécialement conçu pour ça: ils n'ont pas de clavier, de souris, d'écran, ont des disques durs immenses et nécessitent des systèmes de refroidissement très performant... Mais dans l'idée, l'ordinateur sur lequel je tape ces lignes pourrait devenir un serveur ^^.

NB : dans la suite de la brochure, lorsque nous parlerons de serveur nous utiliserons le mot 'ordinateur'.

Lorsque l'on se connecte à internet, on se connecte à ce réseau d'ordinateurs en passant par au moins trois ordinateurs : celui sur lequel on lance un navigateur internet, la box internet sur laquelle on est connecté·e et l'ordinateur de notre **fournisseur d'accès internet**, qui fait le lien entre notre box et le reste du réseau.

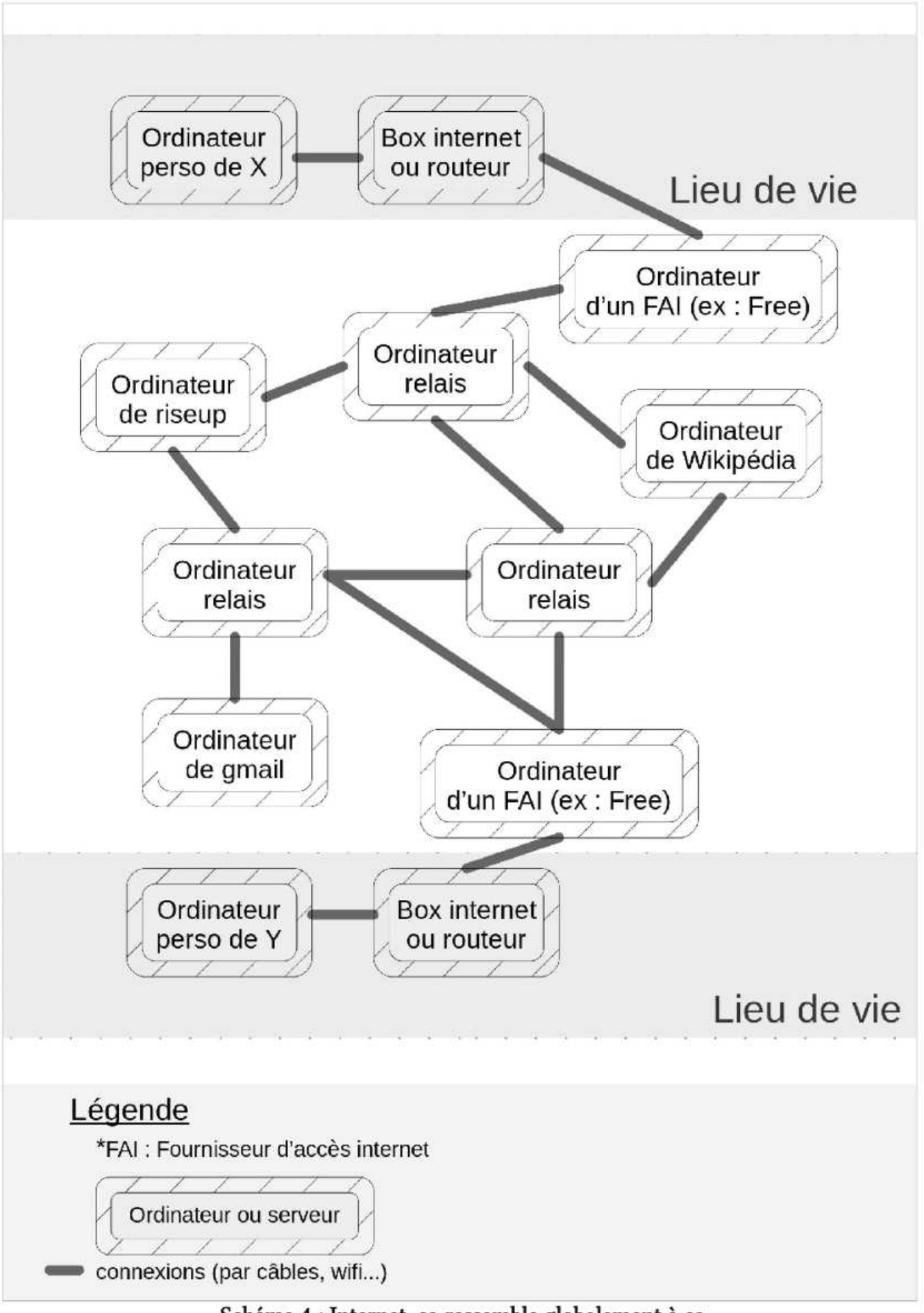


Schéma 4 : Internet, ça ressemble globalement à ça

Comment ça fonctionne?

Un site web

Un site web c'est un fichier qui est tout le temps dispo sur un ordinateur.

Quand je veux accéder à un site web (Wikipédia par exemple), voilà ce qu'il se passe : la demande passe par ma box pour arriver à l'ordinateur de mon fournisseur d'accès internet. L'ordinateur regarde où est le site de Wikipédia sur le réseau. Il va le chercher sur l'ordinateur de Wikipédia et il le ramène sur ma mémoire vive pour que je puisse le lire sur mon ordinateur.

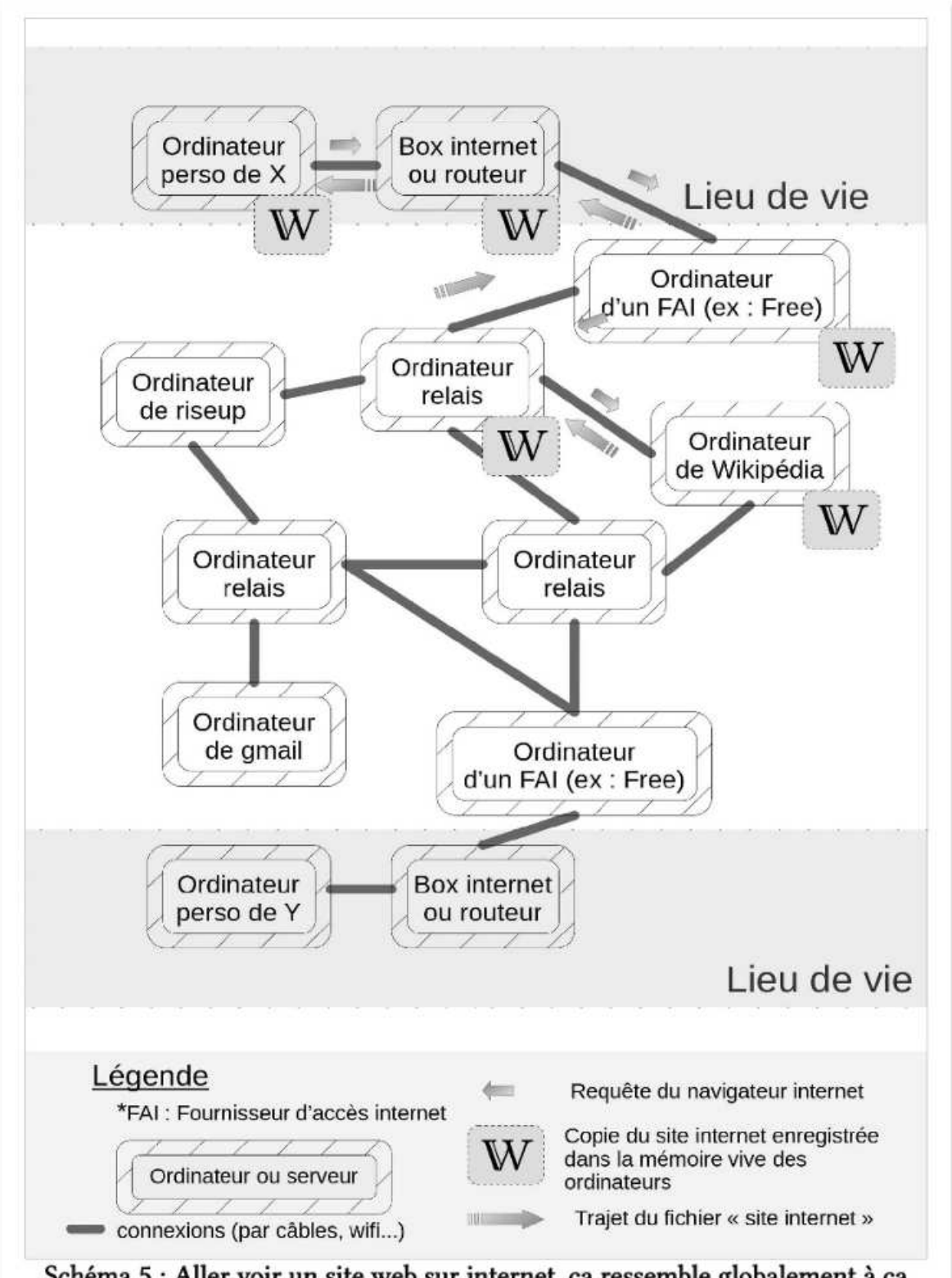


Schéma 5 : Aller voir un site web sur internet, ça ressemble globalement à ça

Un mail

Comme on peut le voir sur le schéma, quand je veux envoyer un mail voilà ce qui se passe : le mail est sur mon ordinateur, il passe par ma box internet puis par l'ordinateur de mon fournisseur d'accès internet. Il est ensuite envoyé à l'ordinateur de mon fournisseur mail puis à l'ordinateur du fournisseur mail de mon/ma destinataire. Le mail passe ensuite par l'ordinateur du fournisseur d'accès internet de mon/ma destinataire puis par sa box internet avant d'arriver sur son ordinateur.

Il peut y avoir d'autres ordinateurs intermédiaires sur le chemin, (« ordinateur relai » dans le schéma et la suite des explication). Quand on communique par mail les informations vont donc passer par plusieurs ordinateurs et beaucoup de câbles (ou antennes wifi, 4G...) avant d'arriver à destination.

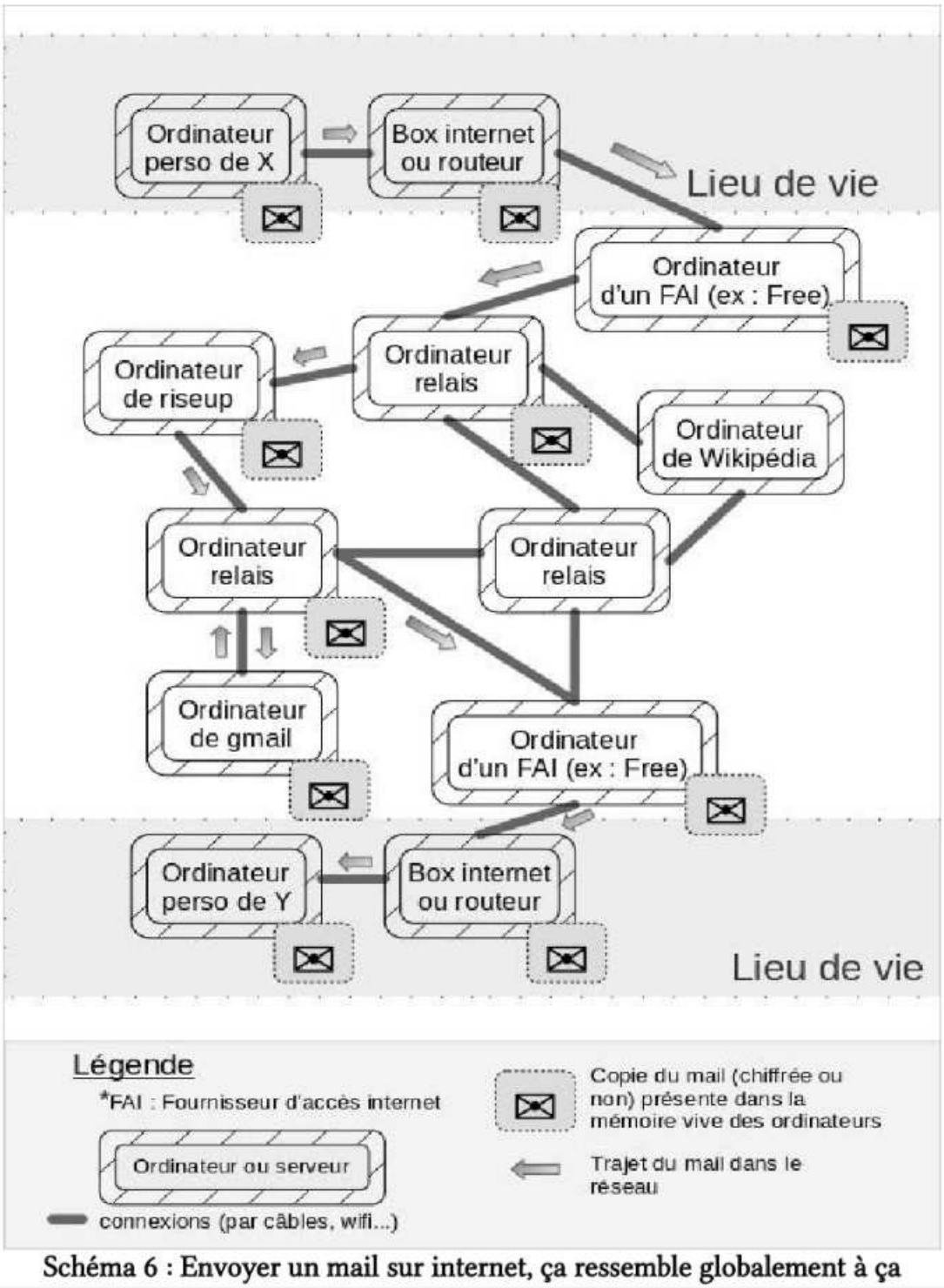


Schéma 6 : Envoyer un mail sur internet, ça ressemble globalement à ça

Où on laisse des traces et comment ne pas en laisser?

Contenu d'un mail

Si on se recentre sur la culture de sécurité, on voit qu'on a laissé des traces : mon mail est passé par de nombreux ordinateurs où il a pu être enregistré. En général les connexions internet sont chiffrées (c'est ce que signifie le 's' de 'https'). Cela veut dire que les copies du mail qui ont été enregistrées sur les ordinateurs relais, les ordinateurs des FAI et les box internet sont chiffrées et donc illisibles pour quelqu'un·e qui accéderait à ces ordinateurs. Par contre le contenu du mail est enregistré en clair sur l'ordinateur de mon fournisseur de mail et l'ordinateur du fournisseur de mail de ma·on destinataire.

Comme pour les logiciels, cela pose la question de la confiance que l'on a dans son fournisseur de mail : Est ce qu'il va lire tes mails? Ou les donner/vendre à d'autres? Si la police lui demande, est ce qu'il va donner accès aux mails? Est-ce qu'il y a certains fournisseurs de mail à qui on peut faire plus confiance que d'autres ? Est-ce qu'il y a moyen de ne pas avoir besoin de faire confiance à son fournisseur de mail ?

Il existe effectivement un moyen de garantir que des mails ne soient lisibles que par leur émetteurice et leur destinataire: le **chiffrement**. Aujourd'hui le chiffrement des mails se fait communément avec un système clé publique/clé privé.

La **clé publique** c'est comme une enveloppe cadenassée, la **clé privée** c'est la clé qui peut l'ouvrir. Tu peux distribuer ta clé publique, c'est comme si tu donnais un stock ou un modèle d'enveloppes cadenassées aux gens. Iels peuvent enfermer le message pour toi dedans (c'est le chiffrement) et tu seras lae seul-e à pouvoir l'ouvrir pour accéder au message avec la clé privée (c'est le déchiffrement).

Informations de connexion

Grâce au chiffrement, le contenu du mail est protégé mais certaines infos sont encore disponibles : ce sont les **métadonnées** (l'adresse de l'émetteurice du mail, l'adresse de son·a destinataire...) et les **informations de connexion** (le fait que telle box internet se soit connectée à l'ordinateur de tel fournisseur d'accès internet pour consulter les mails liés à telle adresse). Les informations de connexions existent dans les échanges de mail mais également lors de la consultation de sites internets : l'information que telle box internet s'est connectée à tel site web, à telle heure...

En cas d'opération de répression, la police a plusieurs moyens d'accéder aux informations de connexions et aux métadonnées :

↣ Scénario 1 : demande de données au fournisseur de mail ou au site web

La police pourrait demander à des fournisseurs mail les informations liées à une boîte mail en particulier. Si les mails sont chiffrés, la police ne peut pas avoir accès au contenu des mails, mais elle a accès aux métadonnées et aux informations de connexion. Elle peut donc identifier précisément la box internet qui a voulu consulter cette boîte mail, et à travers son identification remonter à son/sa propriétaire.

Cet enjeu de sécurité est particulièrement important pour les échanges de mail , parce que les métadonnées et les informations de connexion permettent de lier des adresses mails entre elles et/ou à une identité civile (via la box internet). Pareillement, la police pourrait demander aux administrateurices d'un site internet (par exemple wikipédia.fr ou paris-luttes.info) de fournir les informations de connexions et donc d'établir qu'une box internet en particulier (possiblement reliée à une identité civile) s'est connectée au site internet, l'heure de la connexion, la configuration du navigateur internet de l'ordinateur qui s'est connecté[68].

↣ Scénario 2 : demande de données au fournisseur d'accès internet

En France, la police peut également demander à n'importe quel fournisseur d'accès internet de fournir les informations de connexion disponibles sur leurs ordinateurs. Sachant que lorsque je navigue sur le web de façon « classique », toutes mes demandes de connexions passent par l'ordinateur de mon fournisseur d'accès internet, l'État ou la police peut donc avoir accès à la liste des sites que je visite, l'heure à laquelle je les ai consultés, etc.

Il existe des outils pour éviter que ces données détaillées soient accessibles à votre fournisseur d'accès internet. L'un d'entre eux est le réseau **Tor** et le navigateur qui lui est associé, TorBrowser. Nous parlons des aspects pratiques de leur utilisation dans la partie suivante et du fonctionnement du réseau Tor dans l'annexe *Naviguer sur internet de manière anonyme... C'est à dire ?*

68 https://fr.wikipedia.org/wiki/Donn%C3%A9e_de_connexion#cite_note-CodeFrDef-3, *Donnée de connexion*, Wikipédia

S'OUTILLER POUR AVOIR UNE UTILISATION SÉCURISÉE DES OUTILS NUMÉRIQUES

On a vu des scénarios d'attaques, des pistes pour s'en protéger, maintenant on a besoin d'outils concrets pour passer à la pratique : des logiciels.

Les logiciels sont amenés à être mis à jours régulièrement, certaines manipulations proposées ici peuvent changer. Cette brochure est écrite en 2022. La version des logiciels utilisée est précisée à chaque fois que l'un d'eux est cité pour la première fois.

CHOISIR SES OUTILS

Pour chaque usage il existe tout un tas de logiciels possibles. Par exemple pour écrire un texte il y a Microsoft Word, Libreoffice, Gedit, etc. Comment choisir ?

Voici quelques propositions de critères à garder en tête pour évaluer un logiciel :

⌨ Critères techniques : est-ce que ce logiciel répond à mon besoin ? Est-ce qu'il me facilite grave la vie ? La réponse à cette question est souvent rapide, mais parfois ça peut déjà demander un peu de travail pour comprendre comment un logiciel peut nous aider.

☂ Critères de sécurité : De quel niveau de sécurité j'ai besoin ? Quelles traces produit ce logiciel, avec qui sont-elles partagées ? Il est aussi parfois possible de compléter un logiciel pas assez sécurisé pour le faire atteindre le niveau de sécurité demandé. Par exemple, si je ne veux pas que Windows partage mes informations, il me suffit de ne jamais le connecter à Internet. (À condition bien sûr que l'usage que j'en fais ne demande pas de connexion.) Autre exemple : Les mails envoyés via la messagerie riseup ne sont pas chiffrés. Mais je peux les chiffrer moi en utilisant un logiciel fait pour ça, pour que ni riseup le fournisseur mail du/de la destinataire n'y ait accès.

♙ Critères politiques : Qui me propose ce service ? Quels sont les objectifs de la personne qui a fait ce logiciel ? Comment le travail fournit pour faire ce logiciel est-il financé (bénévolat, dons, logiciel payant, vente de publicité, etc) ?

La première source d'information à propos des logiciels est souvent leur propre site de présentation. Et c'est souvent assez facile à trouver. Par exemple Thunderbird est présenté sur le site web /www.thunderbird.net/. On arrivera souvent très vite à savoir s'il s'agit d'un logiciel libre (« free software » en anglais). Quand c'est le cas, c'est plus facile d'avoir confiance dans la communication qui est faite autour de ce logiciel. Sur ce site on trouvera aussi sûrement des informations sur les personnes qui fabriquent ce logiciel et leur modèle de financement.

Parfois ces informations ne sont pas suffisantes, et d'autres ressources sont nécessaires : Wikipédia, forums, presse, autres sites internet.

Pourquoi Tails (version 5.11) ?

La partie théorique a présenté différents scénarios d'attaques et des manières de s'en protéger (par exemple en chiffrant ses mails ou en écrasant des fichiers). Il y a des logiciels qui permettent de faire ça et on pourrait décider de les installer un à un sur l'ordinateur qu'on utilise tous les jours. Mais il existe également des communautés qui ont développé des systèmes d'exploitation qui rassemblent pleins de logiciels utiles pour se protéger et protéger son utilisation de l'informatique. L'un de ces systèmes d'exploitation s'appelle Tails. Il est conçu pour être installé sur une clé usb. Quand on l'installe, on installe en même temps tout un tas de logiciels qui permettent de chiffrer ses mails, d'écraser un fichier, etc.

C'est la boîte à outils qu'on a choisi de présenter dans cette brochure. On peut regarder par rapport aux critères du paragraphe précédent si ça colle ou pas :

⌨ Critères techniques: à partir des scénarios d'attaques exposés, on a identifié des besoins :

- ❒ Pouvoir écraser un fichier
- ❒ Chiffrer ses mails
- ❒ Utiliser Internet anonymement

Tails fournit des outils pour y répondre, ainsi que de nombreux autres. Ces besoins ne sont peut être pas les vôtres, mais ce seront ceux qui vont servir d'exemple. À vous d'identifier vos besoins et de trouver les outils qui y correspondent.

☂ Critères de sécurité : C'est du logiciel libre, spécifiquement pensé pour répondre aux enjeux d'anonymat et de protection des données. Ça donne la possibilité d'augmenter le niveau de sécurité.

🐧 Critères politiques : Tails est développé par une association, financée principalement par des dons de particuliers[69] mais aussi des dons d'organisations.

Tails rassemble plein de logiciels et on pourrait faire le même travail de recherche pour chacun des logiciels qu'on souhaite utiliser. On va le faire un peu dans la suite du texte, mais on vous invite aussi à vous poser la question de votre côté et à vous renseigner pour les logiciels dont vous avez l'usage. Dans la documentation de Tails vous trouverez une liste tous les logiciels inclus et les liens vers leurs sites web[70].

Les prochains paragraphes présentent Tails et décrivent comment l'installer sur une clé usb.

69 Pour faire un don, c'est par ici ! → https://tails.boum.org/donate/index.fr.html
70 https://tails.boum.org/doc/about/features/index.fr.html, *Fonctionnalités et logiciels inclus*, Tails

Spécificités de Tails: The Amnesic Incognito Live System

Live System

Tails est un système spécifiquement conçu pour être installé sur une clé usb. Cette clé usb est ensuite branchée à un ordinateur et par une manipulation on fait démarrer le système d'exploitation présent sur la clé (Tails) plutôt que celui présent sur le disque dur de l'ordinateur (par exemple Linux ou Windows).

Incognito

De plus, on dit de Tails que c'est un système d'exploitation incognito car il est spécifiquement conçu pour protéger l'anonymat de ces utilisateurices, notamment dans leurs usages d'internet.

Amnesic

Enfin, Tails est présenté comme un système amnésique : il ne laisse aucune trace de son passage sur l'ordinateur utilisé pour le faire tourner et par défaut les documents créés pendant une session d'utilisation ne sont pas enregistrés sur la clé usb mais restent sur la mémoire vive. Ainsi, la clé reste dans son état initial. Dès l'extinction de l'ordinateur il ne reste aucune trace de son utilisation.

Il est possible de contourner ce comportement pour enregistrer quand même des documents ou des paramètres sur une clé Tails en créant un dossier particulier : la persistance. La création de ce dossier est décrite plus loin.

Installation de Tails 5.11

La solution d'installation décrite ici demande d'avoir déjà accès à une clé USB avec Tails installé dessus. Elle permet d'obtenir une 2eme clé Tails à partir de cette première. Si vous n'avez pas accès à cette première clé, les instructions d'installation diffèrent un peu. Vous pouvez les trouver facilement dans la documentation de Tails[71].

Démarrer tails

Par défaut, l'ordinateur qui démarre (qui « boot » en anglais) va chercher un système d'exploitation sur le disque dur. La première étape est donc de lui indiquer d'aller chercher le système d'exploitation sur la clé à la place. Pour ça, il faut intervenir au démarrage de l'ordinateur pour accéder au *boot menu* en appuyant sur une touche juste après avoir appuyé sur le bouton de démarrage de l'ordinateur. Cette touche dépend des constructeurs et des modèles.

71 https://tails.boum.org/install/index.fr.html *Installer Tails*, Tails

Voici une liste pour les modèles courants, trouvée dans la documentation de Tails[72] :

Acer	F2, F9, F12, Échap
Apple	Option
Asus	Échap
Clevo	F7
Dell	F12
Fujitsu	F12, Échap
HP	F9
Huawei	F12
Intel	F10
Lenovo	F12
MSI	F11
Samsung	F2, F12, Échap
Sony	F10, F11, Échap
Toshiba	F12

N'hésitez pas à répéter les appuis sur cette touche, c'est pas toujours évident d'appuyer au bon moment du démarrage.

Donc pour démarrer votre clé Tails il faut donc, dans l'ordre :

1. Brancher la clé Tails sur l'ordinateur éteint.
2. Allumer l'ordinateur. Appuyer immédiatement plusieurs fois sur une touche d'accès au menu de démarrage identifiée dans le tableau précédent.
3. Si l'ordinateur démarre comme d'habitude ou renvoie un message d'erreur, éteindre à nouveau l'ordinateur et répéter l'étape 2 pour chacune les touches possibles identifiées dans le tableau précédent.
4. Si un menu de démarrage avec une liste de périphériques apparaît, sélectionner votre clé USB et appuyer sur Entrée.
5. Si l'ordinateur démarre sur Tails, un écran de démarrage apparaît et Tails démarre automatiquement après 4 secondes.

Ça peut être un peu laborieux de trouver le menu de démarrage de votre ordinateur mais pas de panique, une fois que vous avez trouvé c'est toujours la même chose !

⚠ C'est une manip qui peut être particulièrement galère. Il y a plein de cas particuliers en fonction de l'ordinateur, du système d'exploitation qui est déjà installé dessus, etc. Ça peut être bien décourageant. Ne perds pas espoir ! Et n'hésite pas à demander de l'aide autour de toi si tu le peux (tata un peu geek, collectif de soutien numérique, forum sur internet, ...).

72 https://tails.boum.org/doc/first_steps/start/pc/index.fr.html *Démarrer Tails sur un PC*, Tails

Écran d'accueil

L'écran d'accueil de Tails propose pas mal de paramètres qu'on détaille pas ici, allez voir la doc[73] ! Le seul paramètre qu'on vous conseille de changer avant la suite c'est la langue et la disposition du clavier, tout en haut du menu.

Cliquez sur Démarrez en haut à droite et c'est parti !

Petite présentation

→ Pour accéder au différents logiciels: menu **Application** en haut à gauche de l'écran

→ Pour accéder aux différents dossiers : menu **Emplacements** en haut à gauche

→ Pour se connecter au wifi : cliquer sur la petite flèche tout en haut tout à droite ▾, puis cliquer sur **Wifi non-connecté ▸ Sélectionner un réseau**.

Création d'une nouvelle clé Tails

1. Connecter la nouvelle clé USB sur l'ordinateur.

   ⚠ Toutes les données sur cette clé USB seront **perdues !**
2. Choisir **Applications ▸ Tails ▸ Programme d'installation de Tails** pour démarrer l'Installeur de Tails.
3. Choisir la nouvelle clé USB dans la liste déroulante Clé USB cible.

   ⚠ Si vous avez plusieurs supports connectés, des cartes SD avec votre système d'exploitation dessus par exemple, choisissez bien votre clé USB ! (ça sent la mauvaise expérience personnelle cette phrase...)
4. Pour démarrer l'installation, cliquer sur le bouton Installation.
5. Lire le message d'avertissement dans la fenêtre de confirmation. Cliquer sur Oui pour confirmer.

L'installation prend quelques minutes. La barre de progression se fige généralement pendant quelques instants pendant la « synchronisation des données sur le disque ».

Une fois l'installation terminée, fermer l'Installeur de Tails. C'est gagné !

UTILISATION DE TAILS : QUELQUES TRUCS DE BASE

Voici quelques unes des fonctionnalités de Tails.

Persistance

Pour pouvoir enregistrer des documents qui resteront sur la clé Tails d'une fois sur l'autre, il faut y créer une persistance. La persistance est un dossier chiffré, protégé par un mot de passe. Ainsi, si quelqu'un·e met la main sur votre clé Tails il peut voir qu'un espace est dédié à l'enregistrement des documents mais ne peux pas y accéder tant qu'il n'a pas votre mot de passe.

L'utilitaire pour faire cela est **Applications ▸ Tails ▸ Stockage persistant**

73 https://tails.boum.org/doc/first_steps/welcome_screen/index.fr.html, *Écran de démarrage*, Tails

Cet utilitaire va vous demander une 'phrase de passe'. C'est un autre mot pour dire 'mot de passe' mais qui insiste sur la nécessité de choisir un mot de passe long. Pour plus de détails voir la partie *Mots de passe* de l'Annexe.

Cet utilitaire va également vous demander ce que vous voulez sauvegarder dans la persistance. Ces choix ne sont pas définitifs, vous pourrez toujours rouvrir cet utilitaire plus tard pour les modifier dans un sens ou dans l'autre. La documentation de Tails conseille de n'enregistrer que le strict nécessaire. Pour réaliser l'ensemble des opérations présentées dans cette brochure, vous avez besoin de pouvoir y enregistrer des documents et la configuration de Thunderbird.

Création et suppression de document

Créer un document

Ça se passe comme d'habitude. Oubliez simplement pas de l'enregistrer dans le dossier appelé « Persistent » si vous ne voulez pas qu'il disparaisse à la fin de la session.

Observer/supprimer les métadonnées

Les fichiers numériques contiennent plusieurs types d'informations. Il y a celles qui nous sont accessibles au premier abord, et qui sont celles qui souvent nous intéressent le plus, qui constituent pour nous la partie principale du fichier (par exemple pour une photo c'est l'image en elle-même). Mais le fichier contient pourtant d'autres informations, dont nous sommes parfois peu conscient·es mais qui peuvent s'avérer très utiles... ou très daaangereuses! Ce sont les métadonnées: l'heure et la date auxquelles le fichier a été créé, par quel utilisatriceur, sur quel système d'exploitation ou bien encore la marque du téléphone qui a pris cette photo, sa géolocalisation au moment où la photo a été prise... Ces métadonnées font partie du fichier et s'envoient-avec lui au moment du partage, de la diffusion sur les réseaux ou de l'envoi par mail.

On peut généralement accéder à une partie de ces métadonnées par l'explorateur de fichier en faisant **clic droit ▸ Propriétés**. Une photo peut par exemple contenir le modèle de l'appareil qui a servi à la prendre, la date et l'heure, voire les coordonnées GPS au moment de la prise dans certains cas.

Dans l'explorateur de fichiers de Tails il est possible de faire **clic droit ▸ Remove metadata** pour créer une copie de ce fichier sans métadonnées.

Écraser l'espace disque disponible

Pour effacer toute trace d'un document sur la clé USB une fois qu'on en a plus besoin, on peut le supprimer (**clic droit ▸ Supprimer de manière permanente**) puis écraser l'espace disque disponible, c'est à dire réécrire des données aléatoires à tous les endroits de la clé où on a pas des fichiers qu'on veut garder. Pour cela, cliquer en haut à gauche sur **Emplacements ▸ Persistent**. Puis faire un clic droit dans l'espace blancs sous les dossiers et fichiers et choisir Écraser l'espace disque disponible.

Attention, cette opération est longue, particulièrement sur un gros disque dur. Elle ne peut pas être faite dans l'urgence.

Se connecter à Internet : Tor

Connexion à Tor

Sur Tails, tout est fait pour que toutes les connexions à Internet passent par Tor. Nous détaillons ici les aspects pratique de l'utilisation de Tor. Pour comprendre pourquoi nous choisissons cet outil et comment il fonctionne vous pouvez vous reporter aux annexes dans la partie *Naviguer sur internet de manière anonyme... C'est à dire ?*

Pour commencer, il faut donc d'abord se connecter au réseau Tor. La page de connexion s'ouvre automatiquement lorsque l'ordinateur est connecté à un wifi, par exemple. La première option (Connexion automatique) suffit à se connecter au réseau Tor. Votre routeur (box) et votre fournisseur d'accès savent alors que vous vous connectez à Tor, et ce sera la seule chose qu'ils sauront. Si vous souhaitez essayer de cacher cette information, il faudra utiliser des 'ponts Tor'. Consultez la documentation de Tails[74], pour comprendre les enjeux de ce choix et comment faire.

Navigateur Tor (tor-browser 12.0.4)

Une fois connecté·e à Tor vous pourrez accéder au navigateur Tor. C'est un navigateur web qui s'utilise globalement comme les autres. En vous connectant à certains sites, une redirection vers un site en « .onion » vous sera proposée. Les sites en « .onion » sont des sites web qui sont accessibles uniquement via le réseau Tor. Ceci offre une couche d'anonymisation supplémentaire. Certains sites proposent ainsi une copie de leur contenu sur un site en ".onion".

Gestionnaire de mots de passe : Keepass XC

Principe

Les mots de passe sont utilisés partout sur le net, pour accéder à de nombreux services. Pour des bonnes pratiques de choix de mots de passe, voir la partie *Mots de passe* des Annexes. Sans entrer dans le détail, on peut cependant retenir comme bonne pratique de:

⚷ Choisir des mots de passe forts. En effet, il existe des logiciels qui visent à trouver les mots de passe automatiquement en les testant un par un. Ces logiciels sont mis en difficultés par la taille (nombre de caractères), la diversité des caractères (minuscules, majuscules, chiffres, caractères spéciaux), etc.

⚷ Choisir des mots de passe différents pour chaque site. En effet, si jamais l'un de ces sites se faisait pirater, l'attaquant·e pourrait réussir à trouver votre mot de passe grâce à ce piratage. Si vous utilisez le même mot de passe ailleurs, ce serait beaucoup plus facile pour ellui de pirater ces différents comptes.

Appliquer ces conseils n'est pas toujours évident car il n'est pas facile de retenir de nombreux mots de passe longs. Un gestionnaire de mots de passe est un logiciel qui nous aide dans cette tâche. Il permet d'enregistrer tout ses mots de passe dans un fichier chiffré, protégé par un unique mot de passe très fort.

74 https://tails.boum.org/doc/anonymous_internet/tor/index.fr.html *Se connecter au réseau Tor*, Tails

KeepassXC 2.6.2

KeepassXC est un gestionnaire de mot de passes inclut dans Tails. Lors de la première utilisation il va créer une base de données de mots de passe. Il s'agit d'un fichier unique où seront rangés tous les mots de passe par la suite. N'oubliez pas d'enregistrer ce fichier dans votre persistance pour qu'il survive à l'extinction du système. Ce fichier doit être protégé par un mot de passe fort.

> On vous conseille d'utiliser ici un mot de passe facile à déduire du mot de passe de chiffrement de la persistance. Perdre ce mot de passe peut vous faire perdre votre accès à pas mal de comptes, c'est probablement quelque chose que vous souhaitez éviter.

Le bouton [+] vous permet ensuite d'ajouter des « entrées » dans votre base de données. Chaque entrée correspond à un mot de passe. D'autres infos peuvent lui être associées pour vous aider à vous y retrouver (identifiant associé au mot de passe, titre, etc). Ces informations sont optionnelles. Le petit dé à droite dans la zone de texte qui permet d'écrire le mot de passe à enregistrer permet de choisir un mot de passe aléatoire. Ça évite de se creuser la tête pour trouver un nouveau mot de passe fort à chaque nouveau site.

Ces entrées apparaissent ensuite dans l'écran principal de KeepassXC et on peut faire **clic droit ▸ Copier le mot de passe** (ou cliquer sur la petite clé de la barre d'outils) pour aller le coller où nécessaire.

KeepassXC se verrouille et redemande régulièrement le mot de passe principal, c'est fait exprès.

ENVOYER UN MAIL ANONYME CHIFFRÉ

Choix des outils

Riseup[75]

Riseup est un fournisseur mail qui permet de créer des boites mails sans les relier à d'autres info (autres adresses mail, numéro de tel, identité civile...). C'est une première étape nécessaire pour une boîte mail anonyme. Il reste les données de connexion, qui pourraient permettre à Riseup d'établir que tel routeur (la box) a demandé le contenu de telle adresse mail. Riseup annonce ne pas enregistrer ces informations, mais il est possible de ne pas avoir à s'en préoccuper en utilisant Tor. La seule chose que Riseup verra alors sera que quelqu'un·e utilisant Tor s'est connecté.e à cette adresse mail.

Créer une adresse Riseup demande à ce que quelqu'un·e qui en a déjà une vous fournisse un code d'invitation.

> ⚠ Au moment de l'écriture de cette brochure, Riseup connaît des problèmes de spam, la fonctionnalité de création de nouveaux comptes a été temporairement supprimée pour un grand nombre de comptes. On ne sait pas quand cette fonctionnalité sera de nouveau opérationnelle. Croisons les doigts...

75 https://riseup.net/

Pour créer un code d'invitation si vous avez déjà un compte :

- Rendez-vous sur account.riseup.net
- Identifiez-vous
- Cliquez sur **Invites** dans le menu de gauche
- Puis sur **Create New Invite**
- Le code d'invitation est composé de 2 blocs de 4 caractères séparés par un tiret

Si personne autour de vous ne peut vous en fournir, ProtonMail par exemple vous donne également la possibilité de créer une adresse mail sans la relier à d'autres informations (autres adresses mail, numéro de tel, identité civile...). ProtonMail a déjà donné des informations de connexion à la police par le passé[76]. Il est donc d'autant plus important d'utiliser Tor pour s'y connecter.

La préférences des autrices et auteurs de cette brochures va à Riseup notamment car il s'agit d'une association dont le modèle financier est basé sur le don[77] et le bénévolat. ProtonMail est une entreprise qui finance les services qu'elle propose gratuitement grâce aux revenus tirés de services payants.

> ⚠ C'est quand même cool que collectivement on diversifie les structures qu'on sollicite et/ou qu'on soutient. La concentration des utilisateurices chez une seule structure est problématique : cela donne beaucoup de pouvoir à cette structure, qui peut finir par avoir le monopole, c'est également une grosse charge de travail pour les personnes s'impliquant dans cette structure, si ce fournisseur arrête de fournir le service en question, tout le monde est dans la merde... Riseup n'est pas la seule structure à fournir des adresses mails anonymes. Le réseau Chatons[78] peut permettre de trouver des fournisseurs alternatifs. Riseup fournit également une liste de fournisseurs militants[79]. Certains fournisseurs mails locaux permettent aussi d'obtenir anonymement une adresse mail. Si vous avez besoin d'une adresse mail temporaire et anonyme pour créer un compte mail vous pouvez utiliser des services comme jitjat.org ou dnmx.org, qui permettent facilement d'obtenir une adresse mail anonyme, mais difficilement de chiffrer ses mails (pas de possibilité d'utiliser Thunderbird, par exemple).

76 · https://www.pcmag.com/news/protonmail-explains-why-it-shared-a-users-ip-address-with-police *'Protonmail s'explique sur le transfert de l'adresses IP d'un de leurs utilisateur à la Police'*, PC Mag, 2021 (un article en anglais mais un peu plus précis que celui en français ci-dessous)
· https://www.numerama.com/tech/736940-protonmail-transmet-des-adresses-ip-a-la-police-4-questions-pour-comprendre-la-polemique.html *ProtonMail transmet des adresses IP à la Police*, Numerama, 2021

77 Si vous voulez faire un don à Riseup, c'est par ici ! → https://riseup.net/en/donate

78 Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires. Cette page permet de trouver les hébergeurs du collectif proposant un service en particulier https://www.chatons.org/search/by-service

79 http://riseup.net/fr/security/resources/radical-servers

Thunderbird 102.9.0

Thunderbird est un gestionnaire de mail. Il permet de recevoir des mails, les trier, en envoyer, de gérer un carnet d'adresses, un agenda, de faire de la discussion instantanée, etc. Il permet également de chiffrer et déchiffrer des mails, ainsi que de gérer un carnet de clés de chiffrement associées au carnet d'adresses.

Thunderbird est un logiciel libre, financé par des dons[80] et du bénévolat. La communauté qui le fabrique est hébergée légalement par une fondation non-marchande : la fondation Mozilla.

Et cerise sur le gâteau : Il est déjà inclus dans Tails !

Mise en place

Création d'une adresse mail anonyme

En passant par le navigateur Tor, créez une adresse mail. Si l'objectif est que cette adresse soit anonyme, n'utilisez pas une adresse que l'on puisse relier à vous : Par exemple, n'y mettez pas votre nom ou votre surnom, ou d'autres info qui vous identifieraient facilement.

Vous pouvez utiliser KeepassXC pour choisir un mot de passe.

Configurer un compte sur Thunderbird

Pour un autre guide de configuration d'un compte sur Thunderbird, vous pouvez aussi aller voir la documentation de Tails[81]

Au démarrage de Thunderbird, entrez les informations concernant votre nouvelle adresse mail.

Dans la première fenêtre on vous demande votre nom complet. C'est le nom qui apparaîtra lorsque que vous enverrez des mails, vous pouvez remplir ce champ comme vous voulez.

On vous demande également de renseigner votre adresse électronique, puis votre mot de passe (c'est le même que celui que vous avez choisi lorsque que vous avez créé votre adresse).

Sur la deuxième fenêtre, les champs sont normalement pré-remplis par Thunderbird qui configure automatiquement les paramètres de connexion en fonction de votre fournisseur mail. Vous pouvez les laisser tels quels. Vous pouvez par contre préciser quel protocole utiliser pour se connecter à votre fournisseur de courrier électronique : soit IMAP, soit POP.

- Avec IMAP, Thunderbird se synchronise constamment avec le serveur et affiche les courriers et les dossiers qui sont stockés actuellement sur le serveur. IMAP est plus adapté si vous accédez à vos courriers électroniques depuis différents ordinateurs.
- Avec POP, Thunderbird télécharge les courriers électroniques qui sont dans la boite de réception sur le serveur et peut ensuite les supprimer du serveur. POP est plus adapté si vous accédez à vos courriers électroniques uniquement depuis Tails et les stockez dans le stockage persistant. Attention toutefois à bien faire des sauvegardes si vous faites ce choix là. Si vous perdez l'accès à votre clé Tails vous n'aurez aucun moyen de retrouver vos mails.

---

80 Si vous voulez faire un don, c'est par ici ! → https://give.thunderbird.net/en-US/?

81 https://tails.boum.org/doc/anonymous_internet/thunderbird/index.fr.html *Envoyer des courriers électroniques et lire des flux avec Thunderbird*, Tails

Une fois que vous avez configuré un premier compte sur Thunderbird, il est possible d'en configurer un deuxième (puis un troisième, un quatrième, etc). Pour cela cliquez sur l'icône menu (trois traits horizontaux) en haut à droite de la fenêtre puis ouvrez la fenêtre **Paramètres des comptes**. Dans le menu de gauche, en bas, cliquez sur **Gestion des comptes** puis **Ajouter un compte de messagerie**. La suite de la procédure est la même que pour la configuration de votre premier compte.

⚠ Si, lors d'une même session Tails vous consultez les différents comptes de messagerie que vous avez configuré sur Thunderbird ; autrement dit si vous ne redémarrez pas votre clé entre le moment où vous consultez vos différentes boîtes mails, il y a un risque faible pour que ces différentes adresses soient mises en lien les unes avec les autres[82].

Et voilà ! Et si vous avez des problèmes pour configurer votre adresse mail sur Thunderbird, n'hésitez pas à faire un tour sur la documentation de Tails[83].

Créer une paire de clés publique/privée

- En haut à gauche cliquez sur votre adresse mail.
- Dans la page qui s'affiche, cliquez sur **Chiffrement de bout en bout**
- OpenPGP est le nom d'un format standard de mail chiffré. Sous le titre OpenPGP cliquez sur le bouton **Ajouter une clé**.
- Sélectionnez **Créer une nouvelle clé OpenPGP** et cliquez sur **Continuer**
- Dans l'écran suivant vous pouvez laisser les paramètres par défaut. La date d'expiration n'est pas une information technique. Elle permet de prévenir vos correspondant·es de ne plus utiliser cette clé après une certaine date, dans l'idée que plus le temps passe plus on a de chance de perdre sa clé privée où qu'elle tombe entre les mains de quelqu'un·e d'autre.
- **Confirmer**
- Retour à l'écran des paramètres : Vérifiez que votre clé est bien sélectionnée.

C'est fait !

Envoi de mail

Envoyer sa clé publique

Thunderbird fournit plein de petites fonctions très pratiques. Dans l'écran de rédaction d'un message une option **Joindre** apparaît dans barre d'outils en haut de l'écran. Cliquez sur la petite flèche à droite de ce mot pour dérouler ce menu. Choisissez **Joindre ma clé publique**. Si vous n'avez pas encore la clé publique de votre correspondant.e, vous ne pouvez pas chiffrer votre mail. Vous devez donc aussi décocher l'option **Chiffrer**, en haut à gauche, ou tenter de la trouver en cliquant sur **Résoudre** dans le bandeau jaune, puis sur **Rechercher des clés publiques**

82 https://tails.boum.org/doc/about/warnings/index.fr.html *Avertissements : Tails est sûr mais pas magique !*, Tails (dans l'onglet protéger votre identité)

83 https://tails.boum.org/doc/anonymous_internet/thunderbird/index.fr.html *Envoyer des courriers électroniques et lire des flux avec Thunderbird*, Tails

en ligne... en espérant que votre correspondante l'ai publiée quelque part sur un annuaire de clés. Vous n'aurez plus qu'à l'accepter, et le tour est joué.

Envoyez votre mail. Votre correspondant·e est désormais en mesure de vous répondre via un mail chiffré !

Enregistrer une clé publique

Bonne nouvelle ! Vous avez reçu une clé publique en pièce-jointe d'un mail. Voilà comment l'intégrer à Thunderbird :

- La clé publique est en général un fichier en **.asc**. Passez votre souris sur le fichier en .asc et faites clic droit **Importer une clé OpenPGP**
- Dans le panneau qui s'affiche choisissez **Acceptée (non vérifiée)** sinon vous ne pourrez pas envoyer de mail avec cette clé. Ce paramètre peut être modifié plus tard depuis le Gestionnaire de clés OpenPGP. La vérification de l'authenticité est décrite plus loin.

Ça y est, cette clé est utilisable dans Thunderbird.

Envoyer un mail chiffré

Lorsque vous envoyez un mail à une adresse mail à laquelle une clé publique est associée, vérifiez simplement que la case **Chiffrer** est bien cochée. Il n'y rien de plus à faire, envoyez votre message. Vous pouvez vérifier qu'un mail a été chiffré par la présence d'une mention OpenPGP et d'un petit cadenas coché en vert.

Vérifier l'empreinte d'une clé

Si la clé publique a été transmise par un mail en clair (donc non-chiffré), il existe une possibilité que cette clé ait été corrompue. Plutôt que de vérifier caractère par caractère que la clé n'a pas été transformée, il est possible de vérifier l'empreinte de cette clé. Cette empreinte est le résultat d'un calcul fait à partir de la clé. Deux clés ne peuvent pas avoir la même empreinte.

Vous pouvez trouver cette empreinte dans le **Gestionnaire de clés OpenPGP** qui est dans les **Outils.** Double-cliquez sur la clé concernée pour voir s'afficher, entre autres informations, l'empreinte de la clé. Récupérez l'empreinte de la clé que vous voulez vérifier auprès de votre correspondant·e. Il faut la récupérer par un autre moyen que les mails, car si le premier transfert a été corrompu, celui-ci pourrait l'être aussi. Le moyen le plus sûr est bien sûr de transmettre cette empreinte à l'oral.

Vérifiez simplement que l'empreinte transmise par la personne utilisant la clé est bien celle que vous avez sous les yeux. Si c'est le cas, vous pouvez cocher la case **Oui, j'ai vérifié cette empreinte en personne** pour vous rappeler que vous avez fait cette opération. Si ce n'est pas le cas, n'utilisez plus cette clé, et essayez de comprendre ce qui a pu se passer.

Conclusion

C'est la fin de cette petite visite de Tails et de quelques usages associés. Tails intègre de nombreuses autres fonctionnalités que vous pourrez découvrir au fur et à mesure de vos besoins.

En particulier il existe un utilitaire permettant de faire des sauvegarde de votre persistance sur une autre clé Tails. L'utilitaire est rangé dans **Applications ▸ Outils système ▸ Back Up Persistent Storage**. Ça vaut vraiment le coup de le faire : une clé USB se perd beaucoup plus facilement qu'un ordinateur, et vous venez de stocker vos accès à votre nouvelle boîte mail uniquement sur cette clé !

Pour conclure

Nous voilà (presque) à la fin de cette brochure (loool). On espère que la lecture n'était pas trop dense et les contenus à peu près compréhensibles.

Si vous mettez un premier (ou un deuxième) pied dans la mise en place de pratiques de sécurité et dans la sécurité informatique à travers cette brochure ça peut paraître un peu vertigineux. On vous invite (encore une fois!) à prendre ça en charge collectivement: ça va être beaucoup plus facile d'intégrer des nouvelles pratiques de sécurité si vous êtes plusieurs à le faire.

On vous invite aussi, si vous avez envie d'apprendre à utiliser les outils numériques qu'on présente et les intégrer dans vos pratiques, à commencer à les utiliser même pour des trucs pas très militants. Parce que c'est en ayant l'habitude de ces outils qu'on évite de faire des bourdes...

Par ailleurs notre brochure n'aborde qu'une partie des enjeux liés à la répression. Pour augmenter son niveau de sécurité individuellement et collectivement, il faut aussi prendre en charge les questions liées aux risques juridiques, se renseigner sur le déroulement d'une garde à vue ou d'une perquisition et sur nos droits dans ce genre de situation, savoir se protéger physiquement en cas de violence policière en manif, ...

Si vous avez des remarques, des retours, des questions, etc, vous pouvez envoyer un mail à brochure-secu@riseup.net.

On vous laisse avec un max d'annexes

A +

ANNEXES

Voici quelques informations supplémentaires qui peuvent vous être utiles.

LES REMARQUES QU'ON ENTEND SOUVENT SUR LA MISE EN PLACE DE PRATIQUES DE SÉCURITÉ ET COMMENT Y RÉPONDRE

Quand on a à cœur de se protéger, de protéger nos luttes et de remettre au cœur des discussions les enjeux autour de la sécurité, on est parfois confronté.es à des remarques qui minimisent l'importance de ces sujets. Voilà quelques éléments de réponses qui pourront vous aider à faire valoir la pertinence de discuter à plusieurs des enjeux de sécurité. Gardez en tête que tout le monde n'a pas les mêmes envies/besoins et que discuter collectivement de ces enjeux ne revient pas à mettre en place les pratiques de sécurité que vous trouvez pertinentes mais plutôt à construire ensemble un cadre de sécurité collectif.

« Moi la gardav'/la prison/les keufs, ça me fait pas peur ! »

La question n'est pas si ça fait peur ou pas mais plutôt quel impact ça a sur la lutte. Si une personne se retrouve en garde à vue ou en prison ça a des conséquences au delà de juste son état psychologique, mental, moral. Ça peut impacter psychologiquement son entourage mais ça implique aussi des risques accrus de surveillance sur cette personne et son réseau, parfois de l'inactivité forcée pendant quelques temps (parce que matériellement c'est dur d'être efficace depuis la cellule d'une prison et qu'un contrôle judiciaire ça restreint les champs d'actions). Ça peut aussi avoir des conséquences matérielles (amendes, mises sous scellés de matériel...) qu'il ne faut pas négliger. La question à se poser ce n'est pas tellement: « est ce que je suis en capacité d'assumer la répression que je risque en faisant telle ou telle action? » (même si c'est une très bonne question à se poser avant d'entreprendre des actions « risquées » ou de s'engager politiquement) mais plutôt « quel coût ça a de mettre en place des pratiques de sécurité? pour quel bénéfice? Quelle stratégie on adopte face à la répression? »

« On a rien à cacher, on fait rien de mal/rien d'illégal »

Malheureusement on ne compte plus le nombre de personnes qui n'avaient rien à cacher ou n'avait rien fait de mal, ni d'illégal, et qui ont malgré tout subi plus ou moins de répression. On parle plus haut dans la brochure de l'affaire des 7 antifas de Lyon[84] [85] mais on peut aussi citer l'affaire des jardins de la Buisserate[86] ou encore les personnes ou organisations ciblées par Déméter[87]. De plus en plus, les intentions, les convictions politiques ou encore l'appartenance à

84 https://www.franceculture.fr/emissions/les-pieds-sur-terre/l-affaire-des-sept-antifas-a-lyon *L'affaire des sept antifas à Lyon*, Les pieds sur Terre, 2020

85 https://www.rue89lyon.fr/2021/11/05/proces-sept-antifas-lyon/ *Le procès de sept antifas à Lyon : récit d'une affaire bancale*, rue89Lyon, 2021

86 https://reporterre.net/Jardins-de-la-Buisserate-a-Grenoble-les-militants-sont-libres-mais-leur-colere-a-grandi *À Grenoble les militants sont libres mais leur colère a grandi*, Reporterre, 2021

87 https://reporterre.net/Demeter-la-cellule-de-la-Gendarmerie-qui-surveille-les-opposants-a-l-agriculture *Déméter, la cellule de la gendarmerie qui surveille les opposants à l'agriculture productiviste*,

certains groupes ou mouvements exposent à de la répression, qu'elles soient répréhensibles ou pas.

De plus, sans forcément être exposé soi-même à la répression, mettre en place des pratiques de sécurité peut aussi servir à protéger des proches avec qui on est en lien en protégeant les informations qu'iels échangent avec nous ou protéger des alliéEs qui auraient besoin de ces pratiques en évitant qu'iels soient les seulEs à les avoir et qu'iels aient donc l'air suspect. Plus on est nombreuses à avoir des pratiques de sécurité, plus celles et ceux qui en utilisent pour se protéger se fondent dans la masse.

Enfin, mettre en place des pratiques de sécurité c'est une compétence qui s'acquiert avec du temps/de l'entraînement. On a plutôt envie d'apprendre à le faire avant d'en avoir besoin. Même si pour l'instant tes activités ne sont pas répréhensibles il se peut qu'elles le deviennent, soit parce que tu changes d'activité pour aller vers des activités plus répréhensibles soit parce que le système politique/pénal dans lequel tu vis se durcit et que l'activité que tu pratiquais jusqu'à présent en toute quiétude devient répréhensible.

« Les moyens de la police/la justice sont trop gros pour pouvoir s'en défendre », « C'est trop dur/complexe »

C'est vrai que quand on commence à se renseigner sur la manière dont la justice et la police nous surveillent et nous répriment, ça peut paraître insurmontable. Et c'est vrai qu'individuellement on ne peut pas être 100% 'étanche', tout·e seul·e on ne peut pas faire en sorte qu'aucune information qui nous concerne puisse être récupérée par l'État, la police ou la justice.

Par contre on peut collectivement faire en sorte que les informations qui nous concernent soient plus difficiles à obtenir, éloigner la possibilité de la répression, rendre plus difficile le travail de la police et de la justice d'État. C'est justement parce que c'est compliqué de s'emparer de ces sujets que c'est important de s'en emparer à plusieurs, pour se répartir le travail et les réflexions, s'entraider.

« Ça ne sera jamais parfait donc ça ne sert à rien »

En effet, ça ne sera jamais parfait. On ne réussira jamais à se protéger de tous les risques. Il existera toujours des failles, des couacs, des ratés. L'idée n'est pas de se prémunir de tous les dangers possibles mais plutôt de décider collectivement des risques qui valent la peine qu'on s'en protège. Soit parce qu'ils ont de grandes probabilités d'advenir, soit qu'ils présentent un gros coût s'ils adviennent, soit parce que c'est peu coûteux de les rendre moins probables. Même si on ne réussit pas à faire descendre à zéro la possibilité de subir de la répression, on peut quand même réduire les risques.

Reporterre, 2020

QUELQUES ÉLÉMENTS D'ANTI-RÉPRESSION

Quand on parle de mettre en place des pratiques de sécurité c'est souvent parce qu'on est ou qu'on s'attend à être confrontéE à de la répression, notamment de la part de la police et/ou de la justice. C'est pour ça qu'au delà d'y connaître un rayon en sécurité informatique et de comprendre les enjeux de la mise en place de pratiques de sécurité en terme de vie d'un groupe, relations, confiance, impacts psychologiques, etc, c'est aussi important de se renseigner sur ce qu'on peut appeler 'l'anti-rep' c'est à dire comment les systèmes policiers et judiciaires fonctionnent, quels sont nos droits et comment les défendre, quels outils juridiques peut-on utiliser et tutti quanti.

On vous propose des ressources sur le sujet dans la bibliographie. Mais on a quand même sélectionné quelques infos d'anti-rep qui nous semblaient particulièrement pertinentes, notamment parce qu'elles sont en lien avec des thèmes/situations qu'on a abordé·es dans la brochure. Et peut-être que pas loin de chez vous il existe des collectifs qui peuvent apporter des informations et du soutien sur ces sujets si besoin[88] !

L'obligation de donner ses mots de passe

La majorité de ce qui suit est tiré d'un article de paris-luttes.infos disponible ici[89].

Lorsque la police entre en possession de matériel numérique (téléphone, ordinateur, tablette ...) protégé par un mot de passe elle peut vous demander de fournir ce mot de passe en vertu de l'article 434-15-2 du Code pénal. Pour faire jouer cet article, il y a tout de même des conditions :

- Il faut que la demande émane d'une autorité judiciaire. En garde à vue il faut donc que les officiers de police judiciaire aient une réquisition écrite fournie par un magistrat (juge d'instruction ou procureur).
- Il faut avoir été prévenu que refuser de donner son code constitue un délit : cela doit apparaître sur un des PV ; en absence de PV, ça pourrait motiver une demande de nullité lors du procès, mais sans garantie de succès....
- Il faut prouver que cette demande a un intérêt pour l'enquête, avec l'existence de données sur le portable ou l'ordinateur qui auraient été « utilisées pour préparer, faciliter ou commettre un crime ou un délit ». Si rien ne permet de soutenir que le téléphone ou l'ordinateur aurait servi pour de tels faits, tu as une bonne raison de ne pas fournir le code de déverrouillage.

  → Par exemple, arrêté.e pour outrage ou rébellion, il parait très peu probable que les données se trouvant dans un portable aient servi à préparer ou faciliter ces délits : ça peut tout à fait justifier, devant les juges, le refus de donner ton code.

  → En revanche, le délit de « groupement en vue de », très souvent motivé pour justifier des arrestations massives en manifs ou lors d'agitations émeutières dans les quartiers populaires, est un motif idéal pour que la police fouille dans les portables ou les ordinateurs...

88 https://rajcollective.noblogs.org/ Site du rajcol, Réseau d'Autodéfense Juridique COLlective.

89 https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018?lang=fr, *Du nouveau sur l'obligation de donner son code de téléphone en garde-à-vue : comment éviter le traquenard, 2021*

Il arrive que ces conditions ne soit pas réunies mais que la police demande quand même les mots de passe : le cadre légal n'est donc pas respecté et c'est possible de s'appuyer sur ça pour refuser de divulguer ses mots de passe. Mais il faut être conscient·e que ça peut être difficile: les interactions avec la police sont stressantes et iels ont tout un tas de moyen de nous mettre la pression (menaces, chantage...)

Par ailleurs, si une enquête à été ouverte et que tu donnes ton mot de passe suite à une demande d'un flic qui ne respecte pas les conditions énoncées plus haut, il n'y a pas de vice de procédure et le mot de passe et les infos auxquelles ils donnent accès sont tout de même utilisables dans le cadre de l'enquête[90].

En cas de refus de donner son mot de passe, si les conditions ci-dessus sont respectées ou dans le cadre d'une enquête, les peines peuvent aller...

En cas de refus de donner son mot de passe, si les conditions ci-dessus sont respectées ou dans le cadre d'une enquête, les peines peuvent aller jusqu'à trois ans d'emprisonnement et 270.000 € d'amende (5 ans et 450 000 € s'il y a une preuve que les infos auraient permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets) même si dans les faits, lorsque des condamnations sont prononcées malgré tout par le juge, elles s'élèvent rarement à plus que des petites amendes. Par ailleurs il semblerait que pour l'instant personne n'est été condamné uniquement pour avoir refusé de donner son mot de passe.

Les fichiers de surveillances: un bon moyen de savoir ce que la police recherche comme information

Pour se protéger efficacement de la répression, c'est utile de savoir quelles formes elle prend. Parmi toutes ses formes nous avons entre autres parlé de la surveillance et du fichage. Ce dernier se matérialise par différents fichiers que nous ne détaillerons pas ici mais qui sont décrits dans l'excellente brochure *La folle volonté de tout contrôler*[91].

Ces fichiers contiennent souvent des 'métadonnées' sur les individus (relations entre les lieux, les individu·es, ...), et donnent des outils aux flics pour mieux savoir où choper des infos, qui arrêter stratégiquement, etc.

L'enquête proposée par Reporterre et Médiapart sur la répression à Bure[92] offre un bon exemple des informations qui peuvent être récoltées et de l'ampleur que peuvent avoir des opérations de surveillance dans des contextes de lutte.

En nous basant exclusivement sur la brochure *La folle volonté de tout contrôler*, nous prenons quand même le temps de vous présenter une matérialisation du fichage pour vous donner une idée des moyens mis en œuvre par l'État : la fiche S.

90 Texte de décision de la cour de cassation concernant un pourvoi sur la divulgation d'un mot de passe : https://www.courdecassation.fr/decision/600fe839e5e8160929976c88

91 https://rebellyon.info/La-folle-volonte-de-tout-controler-MaJ-et-23573 , La folle volonté de tout contrôler, Caisse de So' de Lyon, 2021

92 Cette note est longue, y a 3 liens différents et le taf de mise en page c'est l'angoisse... Allez plutôt chercher les réf dans la biblio, c'est page 74. <3

Fiche S :

C'est un sous-fichier du Fichier des Personnes Recherchées (FPR) qui un fichier commun à la police nationale et à la gendarmerie nationale et concerne 580 000 personnes. Dans le FPR on trouve notamment les fameuses fiches 'S' pour Sûreté de l'état, qui concerne les personnes à surveiller. Le FPR est consulté de manière quasi-systématique lors d'un contrôle de police et contient des renseignements sur la personne et un volet 'conduite à tenir' qui décrit l'attitude à adopter par les flics en présence de cette personne (ex: l'interpeller ou au contraire tenter discrètement de récolter des informations sur elle (domicile, occupations, moyens de locomotion, téléphone, vêtements, photos...) et/ou sur les personnes qui sont avec elle, contacter le service qui a créé la fiche, etc).

NAVIGUER SUR INTERNET DE MANIÈRE ANONYME... C'EST À DIRE ?

Nous avons parlé dans la partie *Comprendre les ordinateurs, internet et tout ce merdier* des traces que nous pouvions laisser sur **internet** et notamment des **informations de connexion** (c'est à dire le fait que votre box internet (possiblement reliée à votre identité civile) s'est connectée à tel et tel site, à telle heure, via tel navigateur internet...). Ce sont notamment ces traces qui nous empêchent d'être anonymes sur internet. Il n'est pas possible d'éviter de créer ces traces, les informations de connexion sont utilisées dans les protocoles à la base du fonctionnement d'internet. Notre seule option est de remplacer les informations nous identifiant par celles d'un intermédiaire. Cet intermédiaire va se connecter à notre place à l'ordinateur avec lequel on souhaite communiquer et nous retransmettre la communication ensuite.

Pour faire ça, on a plusieurs options. Ici, on va présenter les VPN et Tor.

Les VPN (Virtual Private Network)

L'idée est de dédier un ordinateur à jouer les intermédiaires : le VPN. Le VPN récolte toutes nos demandes de connexions, se connecte par exemple aux différents sites web auxquels on veut accéder, et nous renvoie les informations.

- Du point de vue de notre fournisseur d'accès, on a fait des demandes de connexion uniquement vers un seul ordinateur : le VPN.
- Du point de vue des sites web, c'est le VPN qui a fait des demandes de connexion. Notre box n'apparaît jamais dans les registres des sites visités.

De plus, un VPN est généralement partagé entre plein d'utilisateurices, ce qui rend d'autant plus difficile leur identification.

Par contre le VPN, lui, connaît tout de notre navigation. Il a accès à la liste des sites auxquels on a souhaité accéder et peut en conserver l'historique. Cela pose à nouveau la question de la confiance qu'on peut lui faire : Pourquoi va-t-il les utiliser ? Pourra-t-il résister à une demande des autorités répressive de récupérer ces informations ?

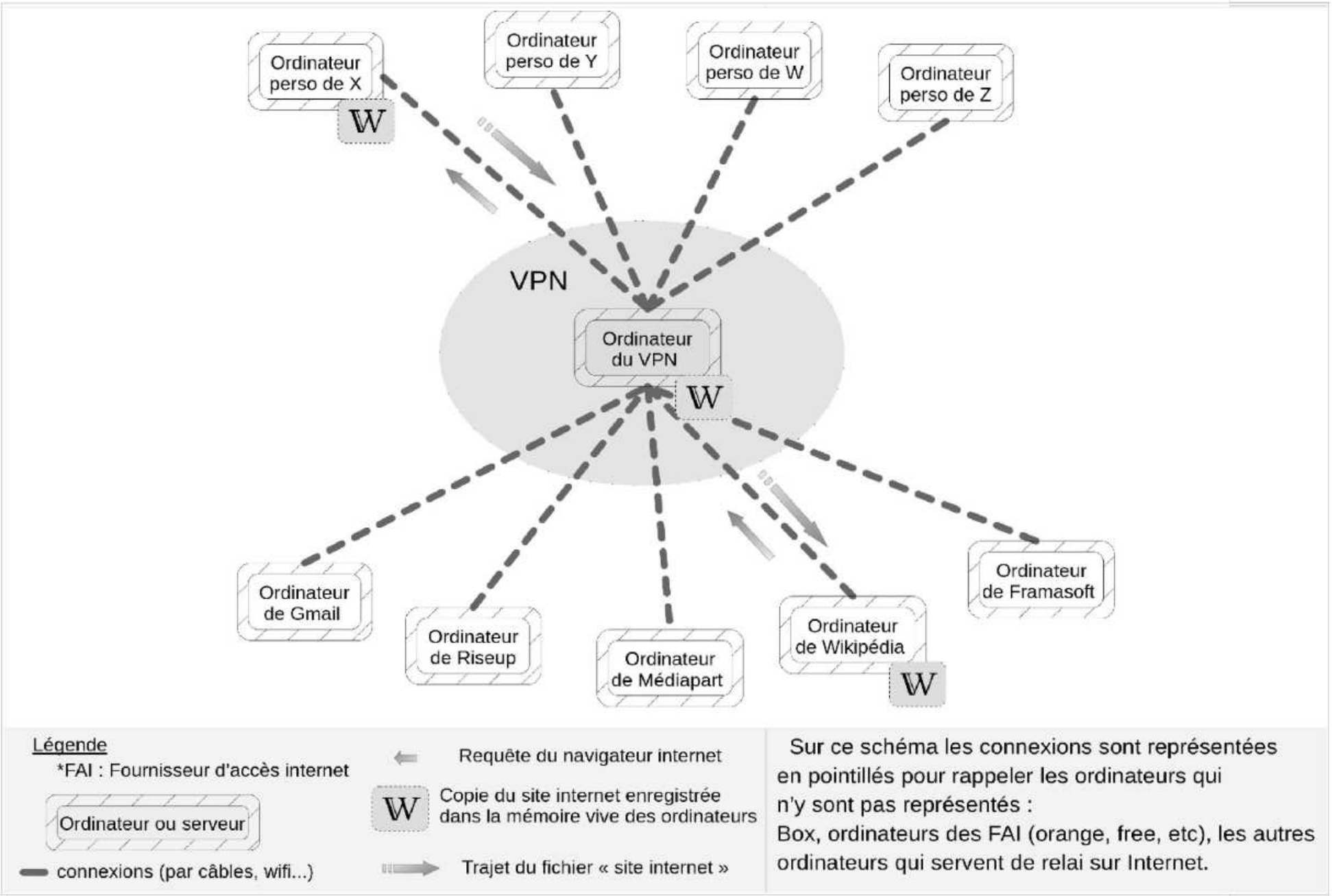


Schéma 7 : Un VPN, ça fait globalement ça

Tor

Tor a pour but de répondre à ce problème de confiance. Tor est un réseau d'ordinateurs qui va jouer les intermédiaires, au lieu d'utiliser un ordinateur unique. Quand on veut se connecter à un site Internet en passant par Tor, notre demande va passer à travers plusieurs ordinateurs du réseau avant d'arriver au site en question. Grâce à un protocole chiffré particulier, chacun de ces intermédiaires ne peut connaître ni l'origine ni la destination de la demande. Il ne connaît de la chaîne que le maillon précédent et le maillon suivant.

Chaque ordinateur du réseau Tor n'a donc pas les moyens de reconstituer notre historique de navigation, contrairement à un VPN.

Le réseau Tor est constitué de plusieurs milliers d'ordinateurs, qui sont hébergés par des bénévoles. Le moyen le plus simple d'utiliser le réseau Tor est d'utiliser le navigateur TorBrowser qui permet d'accéder au web.

Pour plus d'explications sur le fonctionnement de Tor vous pouvez vous référer au guide d'autodéfense numérique[93].

⚠ Dans le cas d'échanges de mails, en utilisant le réseau Tor, seules les données de connexions entre mon ordinateur et mon serveur mail sont cachées. La police peut par exemple savoir que ces deux boîtes mails ont échangé des mails mais elle ne peut pas relier ma boîte mail à mon ordi et donc à moi.

⚠ Si je me connecte via Tor à mon compte Mediapart qui est en lien avec mon adresse mail professionnelle ou avec ma carte bleue, le lien avec mon identité civile est possible.

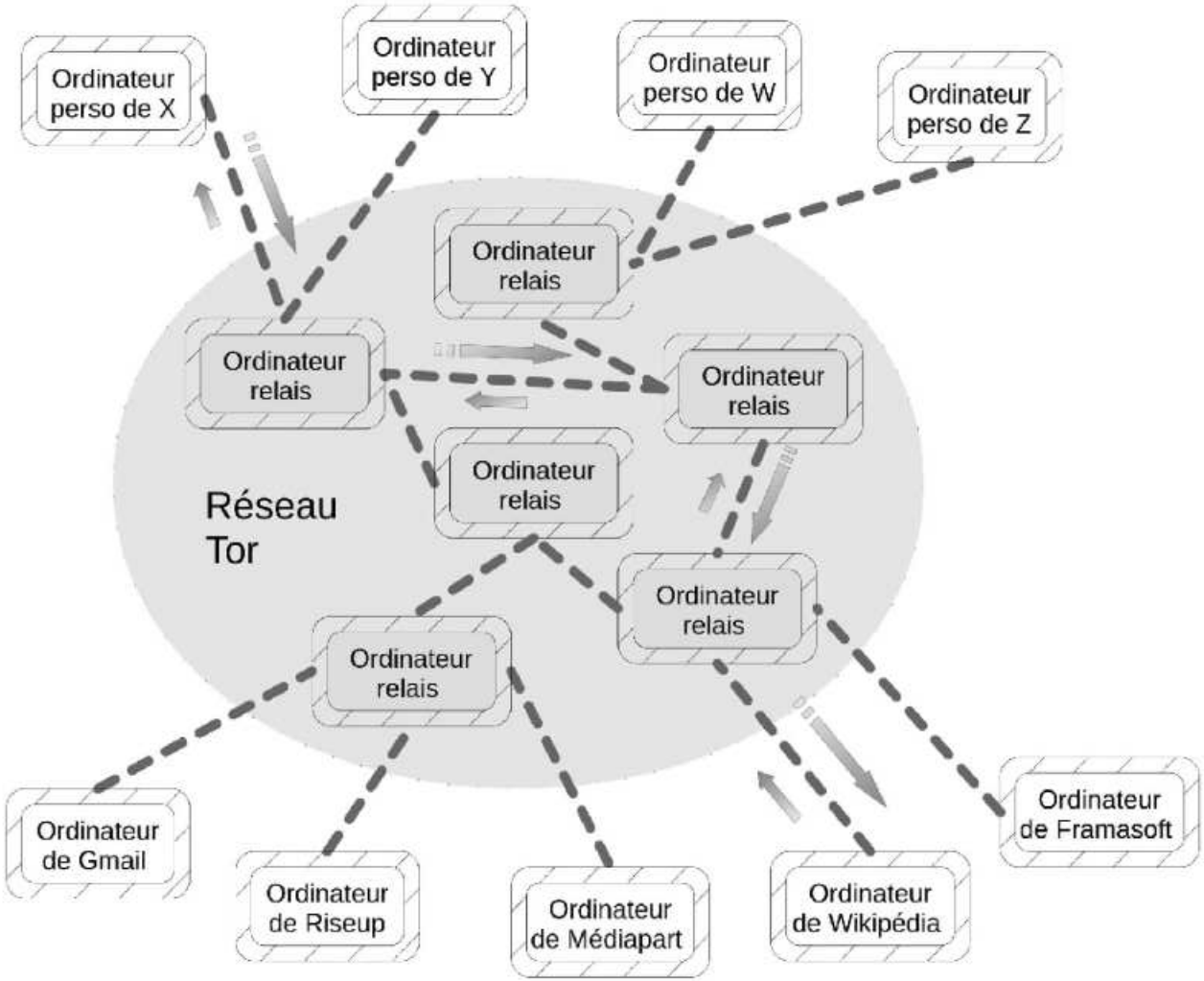
Fingerprinting

Les informations de connexions ne sont pas les seules qui permettent d'identifier un.e utilisateur.ice. Lors de la navigation sur le web, tout un tas d'autres informations sont partagées avec les sites visités : le nom et la version du navigateur que j'utilise, le système d'exploitation que j'utilise, la taille de la fenêtre de navigation, etc, etc. Ces informations sont collectées initialement pour adapter les pages web au support sur lequel elle seront vues. Il se trouve qu'aujourd'hui, avec la quantité d'informations récoltées, il est souvent possible de les recouper pour identifier un outil de navigation (un ordi, un smartphone...) unique. C'est ce qu'on appelle le **fingerprinting.** Ces informations ne permettent pas en elles-même de remonter directement jusqu'à l'identité civile de l'utilisateur.ice, mais elle permettent théoriquement de reconstruire l'historique de navigation d'une personne. Ce travail est facilité par le fait que de nombreuses pages web utilisent les service de GAFAM qui du coup ont accès à ces informations depuis un peu partout sur le web[94]. Des pans de cet historique peuvent permettre de remonter jusqu'à une identité civile. Schéma 8 : Tor, ça fait globalement ça

93 https://guide.boum.org/tomes/2_en_ligne/1_comprendre/7_routage_en_oignon/

94 https://www.statista.com/statistics/1258557/web-analytics-market-share-technology-worldwide/ Google fournit des services d'analyse des visites à presque 75% des sites internet

Schéma 8 : Tor, ça fait globalement ça



Légende

*FAI : Fournisseur d'accès internet

Ordinateur ou serveur

connexions (par câbles, wifi...)

Requête du navigateur internet

Trajet du fichier « site internet »

Sur ce schéma les connexions sont représentées en pointillés pour rappeler les ordinateurs qui n'y sont pas représentés :
Box, ordinateurs des FAI (orange, free, etc), les autres ordinateurs qui servent de relai sur Internet.

En général, les VPN ne cachent pas du tout ces informations et ne sont donc pas efficaces pour lutter contre cette surveillance. En revanche Tor-Browser, le navigateur qui permet facilement de naviguer sur le web via Tor cache une partie de ces informations[95]. Sans configuration particulière, les clés Tails sont particulièrement proches les unes des autres. Elles permettent donc encore mieux de se protéger de cette technique d'identification.

MOTS DE PASSE

Les mots de passe sont très utilisés en informatique pour vérifier que la personne qui souhaite accéder à certains documents ou certaines fonctions est bien légitime à le faire. On en parle plusieurs fois dans la brochure, mais vu leur omniprésence sur le web, on s'est dit que ça valait le coup de faire un point un peu complet là-dessus.

Comment choisir un mot de passe

Difficile à deviner

Un bon mot de passe, c'est un mot de passe qui va être difficile à deviner. Dis comme ça, il semble qu'il y a pas mal de possibilités. Par exemple je pourrais choisir le mot « coussin » comme mot de passe d'accès à ma boîte mail. Si je demande à 2 ou 3 ami·es d'essayer de trouver mon mot de passe, il y a peu de chance qu'ielles réussissent, même en essayant de nombreuses fois. Sauf qu'un ordinateur est capable de tester des milliers de possibilités par seconde ! Sachant que les humain·es retiennent bien les mots de leur langage, quelqu'un·e qui programme un ordinateur pour qu'il devine des mots de passe va commencer par lui faire tester tout les mots du dictionnaire. Et voilà, en moins d'une seconde, mon mot de passe est deviné.

Pour me protéger de ce type d'attaques (les attaques par dictionnaire), je peux complexifier mon mot de passe en y ajoutant des majuscules, des caractères spéciaux, des chiffres, etc. Bref, en faisant en sorte qu'il ne soit dans aucune liste pré-établie. Mais attention, avec ses milliers de tentatives par seconde, un ordinateur peut toujours deviner un mot de passe trop court en testant toutes les possibilités ! Pour me protéger de cette possibilité, il faut utiliser un mot de passe long[96] (min 12 caractères, plutôt 16, bien autour de 20-22, 34 c'est balèze, 57 c'est dingo, 482 c'est MORTEL ! Moi comme mot de passe j'utilise l'intégrale du Seigneur des Anneaux[97], mais bon... Laisse tomber pour arriver à le taper sans faire d'erreurs).

Donc un mot de passe difficile à deviner c'est un mot de passe :

1. Long
2. Avec pas uniquement des minuscules
3. Original (pas *mot2passe*)

95 https://blog.torproject.org/browser-fingerprinting-introduction-and-challenges-ahead/ *Browser Fingerprinting: An Introduction and the Challenges Ahead*, gk, 2019

96 https://www.security.org/how-secure-is-my-password/ (c'est un site de test de mot de passe. C'est pas aussi simple qu'annoncé, mais ça donne une idée)

97 Mince, maintenant tout le monde connaît mon mot de passe...

Facile à retenir

Il faut éviter au maximum d'utiliser le même mot de passe pour plusieurs usages. En cas de compromission de l'un de mes mots de passe, ça évite qu'ils soient tous compromis. Cette compromission peut arriver si un ordinateur devine mon mot de passe en faisant de nombreuses tentatives par exemple, ou lors d'une communication qui serait sur écoute. Mais ça peut aussi arriver si l'un des sites sur lequel j'utilise ce mot de passe se fait pirater.

On a donc besoin de nombreux mots de passe, dans l'idéal simples à retenir pour ne pas avoir à les écrire quelques part. (Ce document pourrait tomber dans de mauvaises mains.)

Une possibilité est d'utiliser une combinaison de mots de la vie courante (voire une phrase). Par exemple 'brocoli nouille cachette miam' ou 'Je dors à la belle étoile' (Même si c'est en soit une vulnérabilité, la capacité à créer de très long mot de passe facilement est plus intéressante que le risque associé). Et on peut toujours ajouter quelques infos au milieu : son chiffre fétiche, quelques caractères spéciaux, un mot dans une autre langue, etc.

On peut aussi utiliser un mot de passe de base que l'on vient modifier pour chaque usage en fonction d'une information lié à un usage. Exemple :

- Mon mot de passe de base : j'aimeleslicornes_bleues!
- Modification pour mon mail sur riseup.net : j'aimeleslicornes_r10t_bleues!

Ma technique c'est : Première lettre de riseup.net, dernière lettre et au milieu le nombre de caractères

Et voilà, j'ai un mot de passe différent à chaque fois mais facile à retenir !

> ⚠ Avoir une règle automatique c'est bien pour s'en souvenir, ça augmente le fait qu'on se tienne à utiliser des mots de passe toujours différents et ça réduit le fait qu'on vienne à le noter partout. Mais si la logique est trop transparente ça peut permettre à l'attaquant de déduire tous les mots de passes facilement.

Utiliser un gestionnaire de mot de passe

Une autre possibilité pour s'aider à utiliser des mots de passe toujours différents et longs est d'utiliser un gestionnaire de mot de passe. (Voir la partie *S'outiller pour avoir une utilisation sécurisée des outils numériques* pour un exemple de gestionnaire de mots de passe : KeepassXC)

Les + :

- Souvent bien chiffré
- Permet de facilement générer de puissants mots de passe aléatoirement pour respecter la règle de un usage = un mot de passe

Les - :

- Pas forcément toujours accessible et donc on peut être tenté·e d'écrire ses mots de passe quelque part
- Un point d'attaque très sensible (*Single point of failure*) : Si quelqu'un·e récupère ma base de donnée et casse mon mot de passe principal, iel a accès à tout d'un seul coup

(mes mots de passe, mes identifiants, des informations sur tous les comptes que j'ai, sur quels services, etc). De plus, KeepassXC (entre autres) est très populaire, et donc très étudié aussi par des attaquant·e·s. Une faille de sécurité serait très vite utilisée (mais du coup il a déjà été corrigé de nombreuses fois et est à priori assez robuste aujourd'hui).

Par exemple, il est possible d'utiliser un gestionnaire qui se met facilement en lien avec les autres outils que l'on utilise (extension pour navigateur, client multi OS, client sur smartphone) pour tous les usages où l'on peut se permettre de ne pas avoir son mot de passe sous la main dans toutes les situations. Et de garder des mots de passe en tête (en respectant les bonnes pratiques) pour quelques mots de passe clé.

QUELQUES OUTILS NUMÉRIQUES SUPPLÉMENTAIRES

On vous a présenté quelques outils numériques qui nous paraissent pertinent, notamment Tails et les logiciels qui lui sont associés, qui couvrent une partie des usages courants de l'informatique. Mais d'autres outils sont parfois nécessaire, notamment des services web.

On vous en propose quelques uns ici et on vous donne des pistes pour en trouver encore d'autres.

Cryptpad[98]

Cryptpad est un service web qui permet de créer et d'éditer des documents en ligne à plusieurs et de manière sécurisée[99]. C'est un logiciel open source, c'est à dire que son code (son fonctionnement) est transparent et accessible à tout le monde.[100]

Ces services sont proposés de manière gratuite ou payante (avec plus d'options) par l'entreprise XWiki dont le modèle économique repose sur les services payants, des dons[101] et des subventions.

Miraheze[102]

Miraheze permet de créer des wikis. Un wiki est un site internet facilement éditable par plusieurs utilisateurices. C'est particulièrement adapté pour avoir un point central d'échange d'informations ou travailler à plusieurs sur un document complexe. Par exemple, Wikipédia est un wiki.

Les wikis créés sur Miraheze peuvent être privés (accès via un compte) mais ne sont a priori pas chiffrés. C'est-à-dire que Miraheze ou la police qui perquisitionne leurs ordinateurs

98 https://cryptpad.fr/

99 Toutes les données d'un cryptpad sont chiffrées dans le navigateur. Ça veut dire qu'aucune donnée lisible ne quitte l'appareil des usager.ères. Même l'administratriceur du service ne peut voir ni les documents ni les données des utilisateurices. Pensez toutefois à verrouiller vos documents par un mot de passe pour les protéger au cas où quelqu'un·e en trouve l'adresse par hasard ou malveillance.

100 Rien à voir, mais WOUUW ! 100e note de bas de page !!! Pompéluuup ! Le-gâ-teau ! Le-gâ-teau !

101 Si vous voulez faire un don , c'est par ici ! → https://opencollective.com/cryptpad/contribute

102 https://miraheze.org/

peut avoir accès au contenu des wikis. La création de compte n'est pas possible via Tor mais peut se faire sans adresse mail.

Miraheze est maintenu par une association anglaise, financée par des dons[103] et du bénévolat. Le logiciel utilisé pour fournir les wikis est MediaWiki, un logiciel libre. C'est le même logiciel que celui qui sert à faire tourner Wikipédia.

Trouver d'autres outils

Dans vos choix d'outils on vous invite à faire attention à la centralisation, c'est à dire qu'un seul outil ou une seule gamme d'outils soit largement majoritaire dans nos utilisations. C'est un des aspects qu'on trouve problématique avec les GAFAM (Google Amazon Facebook Apple Microsoft) et il s'agirait de ne pas retomber dans le même travers lorsqu'on choisit de se tourner vers des alternatives. Si par exemple on se met toutes à utiliser exclusivement Riseup comme fournisseur de mail, le jour où Riseup arrête de fournir ce service (pour une raison ou une autre) on est un peu dans la panade. C'est aussi un point sur lequel l'équipe de Framasoft appelle à la vigilance dans une annonce qui s'intitule *Déframasoftisons internet*[104] et qu'on vous invite à lire. C'est aussi, entres autres, pour cette raison qu'on vous propose d'aller faire un tour sur un de ces deux sites internet qui répertorient des alternatives aux fournisseurs d'outils numériques dont nous avons l'habitude.

Les CHATONS (Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires)[105]

C'est un site en français qui propose des alternatives aux GAFAM pour tout un tas d'usages, en détaillant pour chaque outil la structure qui est derrière, sa localisation, son modèle financier, etc. Le site existe depuis 2016 et fait suite à la campagne dégooglisons internet[106], menée par Framasoft.

Prism Break[107]

C'est un site qui lutte contre les programmes type PRISM[108], et qui répertorie les logiciels recensés comme faisant du fichage et/ou et la surveillance en proposant leurs alternatives. Le travail est fait pour les téléphones, les ordinateurs, mais également pour les réseaux. Il est en open source, et financé notamment par des dons de particuliers.

---

103 Pour faire un don , c'est par ici ! → https://donate.miraheze.org/

104 https://framablog.org/2019/09/24/deframasoftisons-internet/ *Déframasoftisons internet*, 2019 (c'est un article hyper chouette, clair, pédagogique et tout, il vaut le coup de détour!)

105 https://www.chatons.org/

106 https://degooglisons-internet.org/fr/, un chouette site pour comprendre les enjeux autour des GAFAMs et les solutions pour lutter contre leur hégémonie.

107 https://prism-break.org/fr/

108 https://fr.wikipedia.org/wiki/PRISM_%28programme_de_surveillance%29 *PRISM, Programme de surveillance*, Wikipédia

PROPOSITION D'ANIMATION D'UNE FORMATION

En se lançant dans cette brochure, on a eu notamment l'envie de proposer un support pour que le plus de monde possible puisse animer des temps de transmission autour des enjeux de sécurité, même sans avoir trop de bagage d'animation de temps de ce genre. Voilà donc une proposition qu'on espère la plus clé en main possible. Elle est issue de temps qu'on a pu organiser ou auxquels on a pu assister, mais aussi de lectures, de témoignages, etc. Mais bon, on s'est pas trop foulé·es non plus, elle suit le déroulé de la brochure (sans les annexes).

Elle est évidemment à adapter, mâchouiller, recréer selon vos besoins, vos envies, vos contextes, ... Bref !

La formation qu'on propose ici peut être animée par plusieurs personnes, à l'attention de 5, 10 personnes grand max, et se déroule sur une grosse journée. On a mis dans le texte qui suit des outils pédagogiques qui nous paraissent pertinents, les objectifs associés, ...

Déroulé de la journée

Histoire d'avoir une idée globale de ce à quoi ça pourrait ressembler :

Matin :

- intro (15 min ~)
- présentation individuelle (20-30 min)
- temps sur la notion de culture de sécurité (20 min ~)
- discussion en petits groupes (1h ~)
- une pause ! (c'est toujours cool les pauses) (10, 15 min)
- étude de cas concret mais fictif (1h ~)
- conclusion du matin (15 min ~)

Après-midi :

- théorie informatique (1h15 ~)
- une pause ! (parce que la théorie fait fondre les cerveaux) (15 min ~)
- choix des outils numériques (15 min ~)
- démonstration de Tails (20 min ~)
- temps pratique d'apprentissage croisé en petits groupes (1h ~)
- temps pratique sur les mails chiffrés (50 min ~)
- conclusion sur l'informatique (5 min~)
- bilan perso (20 min~)
- conclusion de la formation et questions (temps indéfini)

Introduction

▷ C'est un temps important pour dire un peu pourquoi on est là. Se présenter en tant qu'animateurice, décrire un peu le déroulement de la journée, les objectifs de cette formation, ...

▷ C'est aussi un moment malin pour donner un peu le ton de la journée, des éléments de cadre : rappeler de ne pas se couper la parole, essayer d'être synthétique, à l'écoute des autres et de soi-même, etc.

▷ L'idée c'est de pas y passer des plombes, mais de lancer une dynamique pour les heures qui suivent.

Présentation individuelle

▷ Quand on a réfléchi à comment ça pourrait se passer une formation, on s'est dit que c'était cool d'expérimenter autre chose qu'un classique tour des prénoms pour se présenter, notamment pour éviter de créer un décalage entre ce qui aurait été fait en début de journée (dire son identité civile) et des réflexions / prise de conscience qui pourrait avoir lieu dans la matinée (genre « j'aurais dû dire un blaze en fait ») mais aussi pour déjà commencer à expérimenter d'autres manières de communiquer et de créer du lien.

▷ On ne donne donc pas son nom en début de journée, mais on peut lors de ce temps inviter les participantEs à réfléchir à comment iels voudraient se présenter si jamais la question venait au cours de la journée (que ce soit son prénom de naissance ou un blaze juste pour aujourd'hui) et présenter ça comme un jeu (c'est pas grave si on se plante).

Les objectifs de ce temps

❄ être dans un temps d'échange plus horizontal

❄ commencer à se connaître et faire groupe

❄ potentiellement savoir que des gens partagent nos envies, nos idées, nos préoccupations

❄ travailler à se reconnaître comme des allié·es

Consigne

Les animateurices proposent des questions auxquelles tout le monde répond par écrit sur des petits papiers.[109]

Les papiers sont mélangés dans un chapeau et lus à haute voix par qui veut.

C'est pas obligé de répondre à toutes les questions.

C'est possible d'avoir plusieurs réponses par questions mais on écrit une idée par papier. (On essaye de pas dépasser la trentaine de papiers à lire en tout sinon ça fait vraiment long à tout lire)

109 Oui c'est un petit dragon. Avouez, c'est marrant... C'est marrant, non ? N... Non ? ... Mignon, alors ?

Exemples de questions

- Pourquoi on fait cette formation (participant.es comme animateurices) ?
- Qu'est-ce qu'on pense avoir en commun avec les autres personnes ici ?
- Comment on se sent vis à vis de la formation ?
- Comment on se sent par rapport à la mise en place de pratiques de sécurité? (de manière générale, celles qu'on met déjà en place, celles qu'on aimerait adopter, ...)
- ...

Culture de sécurité : définitions, exploration

Culture de sécurité

▷ Ce temps est un temps de transmission théorique. L'idée, c'est d'aller piocher dans la partie *Culture de Sécurité : kézako ?* autant qu'on veut, sachant qu'elle peut être globalement assez fluide à transmettre en l'état.

▷ Sachant que c'est du théorique, on trouve ça cool d'être quand même dans de l'échange, en posant par exemple des questions qu'on trouve intéressantes à poser aux personnes qui écoutent pour qu'elles creusent un peu en elles-même des pistes de réponse, genre demander aux gens leur rapport à la sécurité, ou quelles traces iels peuvent laisser au quotidien, etc.

Les objectifs de ce temps

❄ Capter des concepts clés dans la compréhension du sujet

❄ Se créer des bases de discussion communes pour la suite

❄ Préparer le terrain pour la compréhension des enjeux de la 2e partie sur l'informatique

Cadre de sécurité pour la journée

▷ À l'issue du temps précédent, ça peut être cool de poser un cadre de sécurité pour les discussions de la journée. Ça peut contribuer à éviter que des informations possiblement sensibles circulent durant la formation, tout en permettant la transmission d'histoires, d'anecdotes, d'expériences qui vont nous aider à contextualiser, à ancrer les connaissances dans le réel.

▷ On rappelle que proposer ça sous le prisme du jeu ou de l'expérimentation, ça aide à dédramatiser les potentielles erreurs et à favoriser l'apprentissage dans un contexte où l'enjeu n'est pas si grand.

Les objectifs de ce temps

❄ Expérimentation de quelles infos sont sensibles ou pas, qu'est ce qui est facile à dépersonnaliser, qu'est ce qu'on peut partager sans crainte.

❄ Potentiellement s'entraîner à utiliser un blaze.

Consigne

Pour protéger les personnes évoquées et ne pas dévoiler inutilement leur identité, tout le monde peut raconter ses histoires de la manière suivante : « un jour, j'ai un·e pote qui ... ». On peut donc être en train de parler de soi ou d'une autre personne, proche, lointaine, célèbre ou non, ce sera toujours à 'un-e pote' à qui arrive l'histoire racontée.

Il y a une exception intéressante, c'est dans le cas où une histoire est déjà publique ou publiée, là c'est quand même chouette de se donner les références pour pouvoir se renseigner par la suite.

Réflexion en petits groupes

▷ Ce temps est un temps pour échanger sur ce qui a été dit et pour se questionner sur les pratiques de sécurité que l'on peut imaginer mettre en place dans sa vie / ses activités, ce que ça implique, ce que ça crée.

▷ Ce temps est pensé pour être fait en petits groupes, de 2, 3 personnes histoire que tout le monde ait le temps de s'exprimer si envie ou besoin.

▷ C'est intéressant que l'animateurice participe un tant soit peu aux discussions et prenne des notes. C'est possible de s'appuyer sur les éléments de la partie *Pistes de réflexions sur la mise en place de pratiques de sécurité* de cette brochure pour relancer la discussion si besoin.

▷ Tips : à la fin, si les participant·es ont du mal à s'arrêter, on peut rappeler que les discussions sont des ouvertures vouées à être approfondies plus tard

Les objectifs de ce temps

❄ Sortir du format « les animateurices parlent et les participant.es écoutent » pour aller vers un temps de partage, où les personnes s'emparent de ce qui est proposé, réagissent, rebondissent...

❄ Rendre plus concrètes les notions abordées et se retrouver autour de questionnements mutuels, échanger sur ses pratiques.

❄ Commencer à s'y mettre !

Consigne

5 axes pour lancer la réflexion (c'est pas obligé de se saisir de tout, y a pas forcément le temps) (ils sont listés plus bas)

ça va durer 40 min

rappeler que c'est chouette de s'appuyer sur du vécu, des partages d'expériences... Parler de ses émotions, c'est rarement des informations sensibles. Mais attention, toujours avec le·a pote qui a fait ou dit les trucs !

On peut prendre des notes dans les groupes (par exemple sur des petites feuilles avec une idée = un papier qui pourront être affichés sur un mur et classées par axe de réflexion pour que tout le monde puisse avoir accès aux discussions à posteriori)

Les axes

1- NIVEAU DE SÉCURITÉ : Quel niveau de sécurité mettre en place dans sa vie / ses activités? Dans quel contexte telle ou telle information est sensible et à protéger? Comment choisir un niveau de sécurité pertinent?

2- ORGANISATION COLLECTIVE : Les impacts de la mise en place d'une culture de sécurité sur l'organisation collective. Dans quel moment / espace collectif la culture de sécurité se manifeste? Qu'est ce que ça complique dans l'organisation collective? Qu'est ce que ça permet ?

3- LA CONFIANCE : Qu'est ce que ça veut dire faire confiance à quelqu'un ? Comment s'articulent la confiance et la mise en place de pratiques de sécurité? Comment nourrir des relations existantes au quotidien tout en maintenant de bonnes pratiques de sécurité ?

4- LES RENCONTRES : Qu'est ce que ça joue dans les rencontres? Comment tisser des liens (sincères / forts) avec de nouvelles personnes sans divulguer d'infos sensibles? Sans amener l'autre à divulguer des infos sensibles?

5- LA TRANSMISSION : Comment transmettre des infos / des expériences / des leçons en continuant à ne pas divulguer d'infos sensibles, en continuant à respecter le niveau de sécurité qu'on s'est donné (individuellement et/ou collectivement)?

Cas concret fictif

▷ Après le temps en petits groupes, on s'est dit qu'un temps en plénière c'était cool pour (presque) terminer la première grosse partie. On vous propose donc de lancer un cas-concret-mais-fictif, sous forme de jeu de rôle (vite fait, quoi), dans lequel les participant·es participent (haha) à une réunion.

▷ Dans la consigne, on a mis en italique un scénario d'histoire fictive à raconter.

Les objectifs de ce temps

❄ Donner des pistes de trucs de sécu à réfléchir pour les groupes d'orga des participant·es

❄ Partager des exemples de pratiques de sécurité à mettre en place concrètement

❄ S'entraîner à relier un cas particulier à d'autres cas connus pour essayer de construire des pratiques de sécurité les plus adaptées possibles.

❄ Faire groupe

Consigne

Scénario (faites vous plaisir pour rajouter moult détails propres à votre contexte local) :

« *Imaginez que juste à côté d'ici, démarre la construction d'un grand projet inutile et imposé. Un groupe de gens que nous sommes aujourd'hui se créé assez vite pour lutter contre ce projet.* »

« *Durant une première réunion faite précédemment, les personnes présentes ont décidé d'actions qui serait pertinentes.* »

C'est possible d'imaginer les actions à l'avance, ou bien de donner à ce moment là 2/3 min pour que chacunE imagine une action possible, à mettre en commun juste après, c'est plus sympa si on a le temps.

« *Toujours pendant cette 1ère réunion, plusieurs personnes ont exprimé l'envie de se questionner sur les pratiques de sécurité à mettre en place au sein de ce groupe. Il est alors décidé collectivement que ce serait abordé lors d'une 2e réunion dédiée.*
On s'est également toustes mis·es d'accord sur le fait qu'au cours de la lutte contre ce sale projet, il pourra y avoir des actions en petit groupe affinitaires, non-discutées/actées en grand groupe. »

L'exercice c'est de faire cette réunion mais sans forcément la faire en entier ou entrer dans le détail. Plutôt passer en revue les différents points qu'il semblerait important de discuter niveau sécurité, d'explorer un peu les questions que ça soulève, les pratiques de sécurité qu'on imagine...

L'objectif c'est pas de prendre de décisions mais plutôt de faire un tour d'horizon des questions que pose la mise en place de pratiques de sécurité au sein d'une organisation et de voir quelles informations il pourrait manquer et qu'il serait nécessaire de connaître afin de prendre des décisions pertinentes.

C'est le moment pour partager des affaires qui se sont passées, sourcer les propos pour pouvoir adapter au maximum les pratiques à la réalité.

Pendant la réunion

▷ On propose que cette réunion fictive soit animée par un·e des animateur·ices de la formation, qui ouvre le jeu avec un petit speech d'introduction et que quelqu'unE prenne des notes et fasse de points de synthèse réguliers, animateurice ou participant·e.

▷ On vous conseille de rassembler en amont de la formation de la matière pour relancer les discussions si jamais elles s'essoufflent: des questions à poser, des références d'affaires similaires si vous en avez, etc.

▷ Quelle place pour des explications techniques (sur l'informatique par exemple) durant ce temps ? Si vous abordez ces aspects l'après-midi ça peut être cool de limiter au maximum les explications techniques qui pourraient émerger durant ce temps pour se concentrer sur les questions stratégiques.

Petit temps de bilan sur la pratique du « j'ai un.e pote qui »

▷ L'idée ici c'est d'ancrer les pratiques de sécurité dans une démarche expérimentale. On a des idées, on teste des trucs et on voit ce qui en sort, à l'inverse d'une culture de sécurité dogmatique qui imposerait certaines pratiques sans les justifier. Et du coup ça peut être chouette de faire un petit bilan sur la pratique du « j'ai un·e pote qui », pour voir comment ça marche (ou pas) pour les participantEs : Est ce qu'on a réussi à l'utiliser ? Comment on l'a vécu ? C'était facile ? Difficile ? Quel impact ça a eu dans nos partage ?

▷ Pour nourrir la discussion on peut questionner les limites de cet exercice :

- faisabilité dans la vie réelle
- même si on limite les logiques de street cred, elles ne disparaissent pas complètement, quelqu'un·e peut encore gagner en charisme en ayant plein d'histoires à raconter... Comment gérer ça ?
- ...

Conclusion du matin

▷ L'idée de ce temps, c'est notamment de réinsister sur des points importants abordés dans la matinée. Petit exemple de condensé si vous galérez à synthétiser :

- mettre en place une culture de sécurité, ça ne peut pas être un truc clé en main, c'est un prisme de réflexion.
- la sécurité, c'est un enjeu collectif, à discuter entre personnes qui s'organisent ensemble. Seul·e, ça marche que pour les activités qu'on a seul·e.
- expérimenter, tester au quotidien sans attendre le moment craignos, c'est le meilleur moyen pour avoir des bonnes habitudes et ne pas se planter une fois qu'il y a des enjeux sérieux.

▷ C'est aussi le moment pour mettre en lien la partie du matin avec celle sur l'informatique. Insister sur le fait que les réflexions de la première partie doivent servir de base à comment on pense nos rapports au numérique, et qu'avoir des pratiques de sécurité en informatique sans avoir une culture de sécurité, sans réfléchir au niveau de confiance, à la segmentation, sans avoir d'esprit critique sur les infos qu'on a envie de diffuser ou pas... ça ne sert pas à grand chose.

Apports théoriques sur les outils numériques

▷ Ce temps reprend les explications que vous trouverez dans la partie *Comprendre les ordinateurs, internet et tout ce merdier*.

▷ Pour faciliter l'assimilation des connaissances, on vous propose de tout expliquer à l'aide d'un 'puzzle' qui reprend les schémas de ce chapitre. Vous pouvez le construire facilement avec du papier des feutres et du scotch. Pour compléter le puzzle, vous pouvez mettre à disposition un glossaire définissant les termes utilisés. On décrit ce puzzle de manière assez assertive, mais comme le reste, n'hésitez vraiment pas à le bidouiller, l'adapter à vos besoins et votre contexte.

▷ Nous ne détaillerons ici que le matériel nécessaire (en encadré) et les petites interventions d'animation, les explications étant déjà présentes dans la partie *Comprendre les ordinateurs, internet et tout ce merdier*. On vous précise à quel paragraphe de cette partie se référer à chaque étape.

▷ Avant de se lancer, vous pouvez faire une petite introduction (amener le fait que l'informatique c'est un outil très utilisé mais difficile à comprendre, les objectifs du temps, ...) pendant laquelle vous faites si besoin un petit état des lieux des connaissances des gens en informatique, pour pouvoir adapter vos explications.

Les objectifs de ce temps

☸ Mieux comprendre comment fonctionnent une partie des outils numériques communément utilisés (ordinateurs, internet, mails...) afin de pouvoir identifier quelles sont les traces qu'on y laisse et qui y a accès.

Ordinateur

▷ Cette installation permet de présenter le contenu de la partie *Ordinateur* > *Matériel*

```
Un ordinateur matérialisé par une feuille et sur laquelle on pose les 3
composants essentiels d'un ordinateur :

- processeur
- disque dur
- mémoire vive
(on peut imprimer des images, les redessiner, sortir des vrais d'un vieil
ordinateur, ...).

On matérialise également différents périphériques :
- une souris
- un écran
- une carte réseau
- un clavier
- une clé USB
```

▷ Cette installation permet de présenter le contenu de la partie *Ordinateur* > *Informations*

```
On symbolise ce qu'on trouve dans un ordinateur en terme de fichiers,
d'information (les composants immatériels) par des papiers.

D'un côté, tous les papiers portent la mention fichier, de l'autre côté on
écrit le fichier représenté.

Il y a des logiciels:
- système d'exploitation
- navigateur internet
- traitement de texte (LibreOffice)
- visionneur d'images
- gestionnaire de boîte mail

Et d'autres types de fichiers:
- un texte
- une photo
- un film
- un historique de navigation
- un index.

Le texte est représenté par plusieurs papiers identiques superposées et
reliées par un trombone. Cela nous servira à matérialiser la manière dont
des copies de ce fichier sont enregistrées à différents endroits de
l'ordinateur.
```

▷ On peut commencer cette partie en plaçant tous les papiers-fichiers sur la table et en laissant les participant·es les regarder, les retourner, et peut être poser des questions sans forcément y répondre.

Protéger les informations qui sont sur mon disque dur, ma clé usb

▷ L'idée ici est de présenter les différents scénario décrits dans le paragraphe *Protéger les informations qui sont sur mon disque dur, ma clé usb*

Lieu de vie

▷ Pareil, on suit les explications du paragraphe *Lieu de vie*

```
Pour visibiliser les différents ordinateurs qu'on peut trouver dans un lieu
de vie, on les symbolise par des feuilles. Ces différentes feuilles portent
la mention « ordinateur » au verso. Il y a :
- une imprimante
-  une box internet
- un smartphone, ...

Les liens (câbles, wifi, ...) entre ces différents ordinateurs peuvent être
symbolisés par du scotch, du fil, …
```

Internet

▷ Quelle surprise ! Cette installation permet de présenter le contenu de la partie *Internet*

```
On symbolise par des feuilles de même taille que précédemment différents
ordinateurs/serveurs :
- l'ordinateur de Wikipédia
- l'ordinateur de Riseup
- l'ordinateur de Gmail
- l'ordinateur de Orange
- l'ordinateur de Free
- la boîte noire de l'état
- et plusieurs autres ordinateurs/serveurs non nommés

On peut matérialiser les connections comme dans l'étape précédente.

On symbolise les différents fichiers qui se trouvent dans ces espaces par
des papiers similaires aux fichiers précédents :
- mail (plusieurs papiers identiques reliées par un trombone pour
matérialiser les copies)
- site web
- historique de visite
- la clé publique et la clé privée
```

Comment ça fonctionne

▷ On peut continuer en expliquant comment marche *Un site web* et *Un mail.*

Où on laisse des traces et comment ne pas en laisser

▷ Puis aller de surprise en surprise en suivant les explication du paragraphe *Où on laisse des traces et comment ne pas en laisser.*

Pratique

▷ Dans cette partie pratique on essaye entre autres de faire toutes les opérations dont on a parlé dans la partie *Comprendre les ordinateurs, internet et tout ce merdier.*

▷ Cette partie demande d'avoir un ordi et une clé usb d'au moins 8go vide par personne.

▷ Dans l'idéal les participant.es viennent avec l'ordi qu'ielles utilisent d'habitude. Ça permet d'essayer de résoudre ensemble les bugs qu'on peut rencontrer plutôt que chacun·e se débrouille avec plus tard.

▷ Vous pouvez venir avec des clés USB en rab au cas où.

▷ On a séparé la pratique en trois parties qui correspondent à trois formes différentes, histoire de dynamiser un peu, parce que ça peut vite être long.

Choix des outils numériques

▷ Dans cette partie on vous propose de reprendre des éléments de la partie *S'outiller pour avoir une utilisation sécurisée des outils numériques >Choisir ses outils.*

Les objectifs de ce temps

❄ Continuer de s'outiller concrètement

❄ Introduire les outils pratiques qui seront utilisés ensuite.

Démo de Tails

▷ Pour présenter Tails vous pouvez vous appuyer sur les parties *Pratique, Choix de Tails* et *Spécificité de Tails: The Amnesic Incognito Live System.*

▷ Il y a pas mal de phases d'attente dans cette démonstration (démarrage de la clé notamment). On peut combler ces moments notamment en expliquant les spécificités de Tails (système amnésique par exemple, ...) ou en profiter pour glisser un mot à propos de la suite en annonçant qu'il va falloir choisir un mot de passe fort et expliquer ce que c'est. Et comme pour la suite on va devoir créer une adresse mail, ça peut-être le moment de commencer à réfléchir à un nom d'utilisateurice.

Consigne

🐉 On peut montrer/expliquer le démarrage et l'installation d'une clé Tails sur un pc.

🐉 Ensuite, chaque participant·e démarre Tails sur son ordi avec l'aide des voisin·es ou des animateurices (ça peut être le moment pour installer Tails sur leur propre clé).

Apprentissage croisé en petits groupes

▷ L'idée est de se mettre en petits groupes avec dans chaque groupe une liste de « missions » à accomplir. Une fois que les participantEs ont trouvé comment faire ces trucs, on redistribue les groupes pour que chacun·e explique ce qu'iel a appris et apprenne des autres personnes.

▷ Si pendant ce temps Tails s'installe sur leur propre clé, dès que l'installation est finie on éteint les clés de départ et on redémarre sur les clés perso. Il faut parfois refaire certaines manip sur ces clés-là pour que chacun·e finissent avec une persistance et une base de données KeepassXC, nécessaires pour l'exercice d'après.

Les objectifs de ce temps

❄ Amorcer une dynamique d'échange d'informations entre pair·es

❄ S'entraîner à retenir et réexpliquer des infos techniques même si on les maîtrise pas complètement

❄ S'autonomiser sur Tails, pour pouvoir le réutiliser plus tard

Consigne

Voici une proposition de liste de missions réparties par groupes. Le détail des missions est dans la partie *Utilisation de Tails : quelques trucs de base*. Cette proposition est à moduler en fonction du nombre de participant·es.

En 2 groupes :

- Groupe 1
  - Configurer une persistance
  - Créer un document
  - Écraser ce document

- Groupe 2
  - Naviguer sur le web via Tor
  - Trouver dans la documentation de tails comment supprimer les métadonnées d'un document
  - Observer et supprimer les méta données d'une image *Penser à préparer une ou des clés usb avec une image bien chargée en métadonnées*
  - Configurer KeepassXC

En 3 groupes :

- Groupe 1
  - Configurer une persistance

- Groupe 2
  - Naviguer sur le web via Tor
  - Configurer KeepassXC

- Groupe 3
  - Créer un document
  - Écraser ce document
  - Trouver dans la documentation de tails comment supprimer les métadonnées d'un document
  - Observer et supprimer les méta données d'une image

S'envoyer un mail chiffré

▷ Une fois les apprentissages croisés en petits groupes terminés, on peut rassembler le groupe pour présenter la suite, rappeler les enjeux d'un mail anonyme chiffré et présenter les outils qu'on va utiliser. Puis on se redivise en petits groupes (accompagnés d'un·e animateurice si besoin).

▷ L'idée de ce temps c'est de s'envoyer un mail anonyme chiffré d'un groupe à l'autre. Le détail des étapes est dans la partie *Envoyer un mail anonyme chiffré.*

▷ Selon les fournisseurs mails que vous voulez proposer aux participant·es, pensez à prévoir le nécessaire pour créer des nouvelles adresses (des codes d'invitation si c'est Riseup par exemple).

▷ L'atelier se termine par la vérification de l'empreinte des clés à l'oral.

Temps de bilan perso

Les objectifs de ce temps

❄ Inscrire cette formation sur un temps individuel plus long, la replacer dans une dynamique d'apprentissage autour de ces questions

❄ Noter ce que cette formation peut/va changer dans ses propres habitudes de vie.

Consigne

🐉 On peut proposer 10 minutes pour se poser individuellement et faire un petit bilan.

🐉 On a rédigé quelques questions auxquelles les participantEs peuvent répondre mais c'est pas obligatoire, ça peut juste être un moment d'introspection sans question, et on peut aussi en trouver d'autres.

- Comment ça va?
- Qu'est ce que j'ai appris, est ce que ça correspond à ce dont j'avais besoin?
- Qu'est ce que j'ai envie d'approfondir comme connaissances?
- À chaud, qu'est ce que j'ai envie de faire de tout ça? Est ce que ces envies sont réalisables? Qu'est ce qu'il me manque?
- Est-ce que j'ai besoin ou envie de transformer des choses dans mes habitudes de vie ? Dans mes pratiques militantes et le niveau de sécurité que je mets en place actuellement ?

Questions et Conclusion

▷ L'idée de ce temps, c'est de finir la formation en laissant les gens partir avec l'envie de s'y mettre sérieusement. Vous pouvez donc redire des trucs marquants de la journée.

▷ Selon l'énergie et la motivation qui restent, ça peut être cool aussi de donner des ptits tips de dernière minute, du genre :

- « *Eh vous avez une clé tail, un mail anonyme, chiffré et d'autres outils cools... C'est stylé !* »

- Pensez à utiliser les outils qui vous ont plu régulièrement, sinon c'est l'oubli assuré ! Ça peut être en se mettant à faire une activité en particulier uniquement sur Tails (lire des articles politisés, aller se documenter, transformer la clé Tails en stockage de dossier un peu sensibles, ou simplement y mettre des recettes de cuisine).
- C'est toujours mieux d'être prêt·e en cas de besoin, et de faire des erreurs quand c'est pas encore trop grave. Et puis si besoin, c'est maintenant possible de refaire une clé, un mail, ...
- S'y mettre, c'est plus facile quand on est plusieurs, pour pouvoir partager les astuces, les galères, les coups de main et les idées. Et c'est encore plus vrai quand on parle d'envoyer des mails chiffrés. Parce qu'encore une fois, on parle de *culture* de sécurité, et une culture ne se fait pas seul:e, sinon ça sert à rien.

▷ Une fois que vous avez fini de dire des trucs, ce temps est aussi le moment où les gens peuvent poser plus ou moins de questions, faire des remarques, ... Faut penser à bien clarifier quand s'arrête le temps de questions et quand commence le temps informel de papote autour de la journée, histoire que celleux qui en peuvent plus puissent se barrer si l'envie y est.

Les objectifs de ce temps

☸ Clore en grand groupe ce temps de formation

☸ Laisser un ptit goût d'empouvoirement qui donne envie d'aller plus loin

Le matériel nécessaire pour la formation

☛ Au moins un espace de discussion avec une table, des chaises, un accès à l'électricité et une connexion internet. Idéalement un deuxième voire un troisième espace similaires pour les moments en petits groupes.

☞ Papier

☛ Stylos

☞ Matériel 'puzzle'

☛ Glossaire

☞ Clés tails

☛ de quoi créer des adresses mail

☞ Ordinateurs (a minima pour les animateurices + possiblement d'autres pour des participant.es qui n'en aurait pas avec elleux)

☛ Multiprises

Réflexions transversales

En construisant le squelette de cette formation on s'est posé plein de questions dont certaines nous paraissaient pertinentes à partager avec vous si vous voulez organiser une formation vous-même.

Tout d'abord on s'est dit qu'on avait envie de faire prendre conscience de la gravité des enjeux de sécurité sans pour autant faire peur ou paralyser. On voulait aussi faire gaffe à ce que personne ne se sente exclu·e, à la ramasse, pas à sa place. On a essayé de faire varier les cadres d'animations (petit groupe | grand groupe, temps où on écoute | temps où on discute...) pour conserver de l'énergie et du dynamisme tout au long de la journée. Ça nous parait important de faire attention à l'énergie du groupe, aux efforts de concentration nécessaires pour suivre la formation. Enfin, on s'est aussi interrogé·es sur l'équilibre entre outiller (faire de la pratique, apprendre aux gens comment se servir d'outils...) et sensibiliser (expliquer le contexte dans lequel on se trouve, faire des temps de théorie et de réflexion...).

Si ça vous dit de vous lancer dans l'organisation et l'animation d'une formation c'est vraiment trop cool ‼ On espère que ça sera un moment sympa 😄

Glossaire Numérique

Ordinateur

Le processeur : c'est la pièce de l'ordinateur qui fait les calculs, c'est à dire fait toutes les opérations qui permettent à l'ordinateur de fonctionner.

La mémoire vive : c'est un composant qui sert à stocker des données quand elles sont utilisées. Leur sauvegarde est temporaire car la mémoire vive se vide entièrement quand on éteint l'ordinateur. L'accès à cette mémoire est très rapide.

Le disque dur : c'est un composant qui sert à stocker de données. Sur le disque dur la sauvegarde est pérenne (les données restent sauvegardées même quand on éteint l'ordinateur). L'accès aux informations qui sont stockées sur le disque dur est plus lent que pour la mémoire vivre.

Une clé USB a le même rôle qu'un disque dur : c'est un espace de stockage pérenne mais plus lent.

Système d'exploitation : c'est un peu comme le 'pilote' de l'ordinateur, le logiciel qui guide le fonctionnement des composants essentiels et des autres logiciels. (Ex : Linux, Windows, Tails...)

Logiciel : fichier dans lequel il y a des instructions.

Index : C'est la « table des matière » du disque dur. Il indique aux différents logiciels (et notamment au système d'exploitation) où sont rangés les différents fichiers.

→ Lorsqu'on **supprime** un fichier, on ne fait que rayer sa mention dans l'index. Tout le contenu du fichier est encore présent dans le disque dur.

→ C'est en **écrasant** le fichier que l'on s'assure que l'ensemble du contenu du fichier a bien été effacé du disque dur.

Métadonnées : les données qui sont dans le fichier mais qui n'apparaissent pas dans son contenu, lorsqu'on l'ouvre normalement. Par exemple, pour un document texte, les métadonnées peuvent comporter le logiciel de création du texte, son auteurice, la date et l'heure à laquelle il a été créé.

On parle également de métadonnées pour des fichiers qui circulent sur internet, par exemple des mails (voir plus bas la définition de métadonnées dans Internet).

INTERNET

Internet : Un système (des câbles, des ordinateurs et des protocoles) qui connecte des ordinateurs entre eux.

Web : Un des usages d'internet qui concerne la consultation de site web. D'autres usages du système internet sont par exemple l'échange de mail ou encore la téléphonie...[110]

Protocole : Un ensemble de normes de communication entre ordinateurs (quelles informations sont échangées, dans quel ordre, etc).

FAI : Fournisseur d'Accès à Internet : L'entreprise ou l'association qui donne à d'autre personnes la possibilité d'accéder à Internet (ex: Orange, Free, Illyse[111]...)

Serveur : Un ordinateur, souvent sans écran ni clavier, utilisé pour maintenir des services internet (site web, distribution de mail, etc).

Tor : réseau informatique mondial qui permet d' « anonymiser » ses connexions à Internet

Chiffrer : transcrire des données dans un « langage » codé accessible seulement aux personnes possédant le code de déchiffrement.

Clé publique/clé privée : paire de fichiers qui sert pour le chiffrement, notamment le chiffrement de mails. Dans la métaphore que nous utilisons dans cette brochure, la clé publique correspond à un modèle d'enveloppe cadenassée et la clé privée est la clé permettant de déverrouiller ce cadenas.

Métadonnées : les données qui sont dans le fichier mais qui n'apparaissent pas dans son contenu, lorsqu'on l'ouvre normalement. Par exemple pour un mail : l'adresse de l'expéditeurice et de la/le destinataire, l'heure et la date d'envoi...

Fingerprinting : Utilisation de certaines métadonnées particulières pour identifier un ordinateur qui navigue sur le web. Ces données rassemblent entre autre le nom du navigateur, sa version, la taille de la fenêtre de navigation, la langue de préférence, etc.

Informations de connexions : Informations datées créées lors d'une connexion entre deux ordinateurs et qui comportent entre autres : des numéros permettant d'identifier l'un et l'autre des ordinateurs, l'heure de la connexion, le navigateur web qui a pu être utilisé pour cette connexion... Les informations de connexions sont souvent enregistrées dans l'un de deux ordinateurs à l'origine de la connexion, mais peuvent également être enregistrées sur des ordinateurs intermédiaires.

110 Pour mieux comprendre la différence entre internet et le web vous pouvez consulter la page Wikipédia suivante ainsi que ses sources: https://fr.wikipedia.org/wiki/World_Wide_Web#cite_ref-4

111 https://www.illyse.net/ Illyse est un FAI associatif sur Lyon et Saint Étienne.

Bibliographie

Voici une petite bibliographie regroupant des sources qui ont été notées tout au long de cette brochure, mais aussi des sources que l'on a pu trouver intéressantes. On a tenté de la regrouper par thèmes. Bonne lecture/audition/visionnage!

Références qui nous ont beaucoup beaucoup servi et/ou qu'on aime particulièrement :

♥ L'Inénarrable, l'Unique *Wikipédia*[112]

♥ *Guide de survie en protection numérique à l'usage des militant·es*, 2021[113]

♥ Tout le dossier de Reporterre et Médiapart de 2020 sur la répression à Bure :
1/3 - La justice a massivement surveillé les militants antinucléaires de Bure[114],
2/3 - L'État a dépensé un million d'euros contre les anti-nucléaires de Bure[115]
3/3 - À Bure la justice a bafoué les droits de la défense[116]

♥ *Guide d'Autodéfense Numérique*, 2023[117]

112 https://fr.wikipedia.org/wiki/Sp%C3%A9cial:Page_au_hasard #page surprise
113 https://infokiosques.net/lire.php?id_article=1849
114 https://reporterre.net/1-3-La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure
115 https://reporterre.net/2-3-L-Etat-a-depense-un-million-d-euros-contre-les-antinucleaires-de-Bure
116 https://reporterre.net/A-Bure-la-justice-a-bafoue-les-droits-de-la-defense
117 https://guide.boum.org/

Répression

- *Étude sur les tué·es de la police*, Bastamag, 2020 : https://bastamag.net/webdocs/police/
- *Rapport sur les violences policières*, ACAT, 2015 : https://www.acatfrance.fr/public/rapport_violences_policieres_acat.pdf
- *Violences policières en France*, Wikipedia : https://fr.wikipedia.org/wiki/Violence_polici%C3%A8re_en_France#Statistiques
- *Rendez-moi mon slip*, témoignages de la répression à Bure, 2021 : https://noussommestousdesmalfaiteurs.noblogs.org/files/2021/05/SLIP_OK.cleaned.pdf ou https://noussommestousdesmalfaiteurs.noblogs.org/rendez-moi-mon-slip-la-version-integrale/

Culture de sécurité

- *Guide de survie en protection numérique à l'usage des militant·es*, infokiosques, 2021 : https://infokiosques.net/lire.php?id_article=1849
- *Confidence. Courage. Connection. Trust. A Proposal for Security Culture*, 2019 : http://aka3xvhiygnchpsbrilphkzbdxtvr6j6pc7hluf6mf2ddruttsikswad.onion/fr/index.html#confidence-courage-connection-trust (en .onion) ou https://www.csrc.link/fr/#confidence-courage-connection-trust
- *Cultures de la Sécurité*, 2004 : https://crimethinc.com/2004/11/01/cultures-de-la-securite
- *The story of how one activist group kept ourselves safe and strong in the face of movement infiltration*, Damage Control, 2015 https://www.infiltration.fail/
- Site intéressant à fouiller, surtout dans la partie ressources, il y a des outils sympas pour comprendre des trucs informatiques : https://laboussole.coop/ressources/

Fichage, surveillance

- *Face à Facebook*, Infokiosques, 2020 :https://infokiosques.net/lire.php?id_article=1725
- *Prism break*, site qui recense des logiciels problématiques et leurs équivalents libres : https://prism-break.org/fr/
- *Contrachrome*, 2022 : https://contrachrome.com/ContraChrome_fr.pdf

Contre-surveillance

- Site qui répertorie les différents dispositifs de surveillance, les endroits où on a déjà retrouvé des dispositifs de surveillance, etc : https://earsandeyes.noblogs.org/fr/
- *La folle volonté de tout contrôler*, 2021 : https://rebellyon.info/La-folle-volonte-de-tout-controler-MaJ-et-23573

OUTILS INFORMATIQUES

- *TuTORiel Tails*, 2022 : https://infokiosques.net/spip.php?article1726
- *Security in a Box*, site de conseils pour protéger ses données, construit pour les défenseurs des droits dans le monde (attention, iels conseillent selon les outils des lecteur·ices, sans faire de critique de l'outil utilisé (logiciels propriétaires, etc.)) : http://lxjacvxrozjlxd7pqced7dyefnbityrwqjosuuaqponlg3v7esifrzad.onion/ (site en .onion) ou https://securityinabox.org/en/ (le site a une version française, mais dont les informations ne sont plus mises à jour)
- *Guide d'Autodéfense Numérique*, 2017 : https://guide.boum.org/
- Site des actualités de Linux et des logiciels libres : https://www.toolinux.com/
- Site qui rassemble des structures proposant des services en ligne libres, éthiques et décentralisés : https://www.chatons.org/
- Site pour comprendre les enjeux autour des GAFAMs et les solutions pour lutter contre leur hégémonie : https://degooglisons-internet.org/fr/
- Plateforme d'hébergement de wikis : https://miraheze.org/fr
- Plateforme de services collaboratifs chiffrés en ligne : https://cryptpad.fr/
- Un livre illustré (et en anglais...) pour comprendre un peu *How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance*, No Starch Press, 1, 2020 (téléchargeable ici : https://fr.annas-archive.org/md5/dc2c6dc8a9fb91baec8d4f8bc7bcb8cf)

POUR ALLER PLUS LOIN

Lieux de ressources disponibles

- Centre de documentation sur la contre-surveillance : https://www.csrc.link/fr/ ou http://aka3xvhiygnchpsbrilphkzbdxtvr6j6pc7hluf6mf2ddruttsikswad.onion/fr/
- Infokiosques en ligne : https://infokiosques.net/
- Imago-TV, plateforme vidéo gratuite de la transition : https://www.imagotv.fr/
- Technopolice, articles, guides pratiques, cartographie des moyens de surveillance et comment s'en protéger : https://technopolice.be/ ou aussi https://technopolice.fr/presentation/
- *Cortecs,* plateforme de ressources sur la zététique/autodéfense intellectuelle : https://cortecs.org/
- *Reporterre*, articles journalistiques sur l'écologie : https://reporterre.net/
- *La quadrature du net*, site de défense des libertés fondamentales dans l'environnement numérique : www.laquadrature.net/
- *Exodus* privacy, un site qui analyse les problèmes de vie privée dans les applications Android : https://exodus-privacy.eu.org/fr/

Outils de la répression

- *Analyse d'un dossier d'instruction antiterroriste*, Infokiosques.net, 2010 : https://infokiosques.net/lire.php?id_article=789
- *Face à l'outil antiterroriste, quelques éléments pratiques*, 2010 : https://infokiosques.net/lire.php?id_article=762
- *Le renseignement français*, Attaque, 2020 : https://attaque.noblogs.org/post/2020/06/14/brochure-le-renseignement-francais/
- Olivier Razac : *Avec Foucault, après Foucault : Disséquer la société de contrôle*, 2008, *Histoire politique du barbelé*, 2009
- *Loi sécurité globale adoptée : résumons*, La Quadrature du Net, 2021 : https://www.laquadrature.net/2021/04/16/loi-securite-globale-adoptee-resumons/
- *Règlement IA : la Commission européenne tend le piège de la reconnaissance faciale*, La Quadrature du Net, 2021 : https://www.laquadrature.net/2021/09/22/reglement-ia-la-commission-europeenne-tend-le-piege-de-la-reconnaissance-faciale/
- *La reconnaissance faciale dans les fichiers de police*, Infokiosques.net, 2020 : https://infokiosques.net/lire.php?id_article=1728
- *L'Envolée*, plateforme de ressources des luttes anti-carcérales : https://lenvolee.net/

Anti-répression

- *Face à la Police / Face à la Justice*, Cadecol, 2016 **(Attention, ce texte commence à dater, certaines informations ne sont plus exactes)** : https://www.actujuridique.com/2eme-edition
- Site du rajcol, Réseau d'Autodéfense Juridique COLlective : https://rajcollective.noblogs.org/

Outils des luttes

- *Mettre fin à l'essentialisme : de l'en-dedans, de l'en-dehors et de l'en-contre*, Aviv & Thomas, 2017 (p 1 à 4 surtout) : https://la-maraude.fr/site/wp-content/uploads/2020/12/Mettre-fin-aE%CC%8C-lessentialisme.pdf
- *Lutter Ensemble - Pour de nouvelles complicités politiques*, Juliette Rousseau, 2018
- Full Spectrum Resistance 1/4 : Se battre et Gagner, Floraisons, 2019 : https://floraisons.blog/full-spectrum-resistance-1-4/

Outils numériques

- *Comment s'organiser en ligne, une brochure pour lutter!*, Rebellyon, 2020 (brochure sortie en contexte confinement) : http://e7nkzth74kcn6j54u6a75pbh2q2yxjsyramuta5z7seix26gnpsq36ad.onion/Comment-s-organiser-en-ligne-Une-brochure-22066 (site en .onion) ou https://rebellyon.info/Comment-s-organiser-en-ligne-Une-brochure-22066

Un immense merci à toutes les personnes qui ont relu notre travail pour leurs précieuses corrections et ajouts.

Big up aussi à toutes les communautés qui développent et mettent à jour les outils numériques dont on parle dans cette brochure et qui font vivre les structures qui les mettent à dispositions.