DEFENSE NUMERIQUE
juin 2023 – maj avril 2024

Ce guide se focalise sur les smartphones et conseil l'usage de Tails pour les ordinateurs.

Tout ce qui est écrit dans ce guide est vérifiable facilement sur internet. Nous vous invitons à le faire et approfondir les sujets que vous trouvez pertinents.
Ce guide à vocation à évoluer : pour le compléter ou en cas d'erreur, de coquille, de doute, envoyez un mail à defensenumerique1312@riseup.net

La partie sur les smartphone reprends la brochure parut en janvier 2023 « Téléphonie mobile Surveillances, répressions, réduction des risques » et accessible sur infokiosk.net
Ce guide s'appuie également sur le « guide de survie en protection numérique à l'usage des militantes » août 2021.
La partie sur tails s'appuie sur le « guide d'autodéfense numérique ».
La sélection d'outils proposée dans ce guide n'est pas exhaustive, pour en savoir plus et se tenir à jour rendez-vous sur privacyguides.org/fr
Le site de surveillance self défense (ssd.eff.org) et celui de security planner (securityplanner.consumerreports.org) valent également le détour.
Pour aller plus loin, vous pouvez lire « The Hitchhiker's Guide to Online Anonymity » avril 2023 par Anonymous Planet.

Notre niveau de sécurité est celui de la personne la moins sécurisée avec laquelle on communique. Inviter à ce qu'il y ait plus de gens à utiliser ces techniques permet également de se protéger dans la masse.

Sommaire :

Téléphonie mobile, rapidement comment ça marche ?

Un téléphone allumé sans mode avion envoie un signal (se connecte) aux antennes proches sans arrêt (qui peuvent déterminer votre position via une triangulation de 3 antennes). L'antenne reconnaît alors la validité de la carte SIM et du téléphone. La carte sim contient un numéro d'identification (IMSI) que l'opérateur vérifie afin d'autoriser ou non les communications avec d'autres téléphones.
Le numéro IMEI est un numéro de série qui identifie de manière unique le téléphone.

Les fadettes mentionnent les numéros, dates, heures et durées de communication. Les opérateurs gardent les « factures détaillées » (ou Fadettes) pendant 5 ans, c'est de la législation fiscale. Ce temps correspond au délai de contestation possible des factures. Mais le cadre légal ne permet en théorie pas aux flics d'en demander l'accès au-delà d'un an.

Tout le matériel réseau est possédé par des entreprises privés qui vendent nos données et collaborent avec les états. Il n'est pas possible de faire confiance au matériel du réseau.

Ce que les flics peuvent faire (On a des éléments de pratiques utilisées dans des dossiers judiciaires ou des lois):

Interceptions administratives et judiciaires
La police peut faire des réquisitions auprès des opérateurs, soit pendant un évènement, soit après coup.
• sur une antenne en particulier : identifiants IMEI et/ou IMSI ayant borné à telle antenne à tel moment.
• sur un téléphone ou un carte SIM spécifique :
- données fournies à l'opérateur : adresse mail, coordonnées bancaires, l'identité
- géolocalisation en temps réel et historique bornage
- historique des cartes SIM mises dans tel téléphone
- liste des téléphones ayant servis à telle carte SIM
- historique des appels et SMS envoyés (mais pas les contenus s'il n'y avait pas de mise sous écoute),
- mise sous écoute en temps réel (cela renvoie en parallèle l'appel sur le téléphone d'un flic)
- les factures détaillées
- les sites consultés (pas toujours possible, et dans beaucoup de cas ne concerne que les domaines visités, pas les pages exactes)
- le code PUK
- en cas de cartes prépayées, la police peut demander où a été vendue cette carte
- etc.
• sur une recherche auprès de chacun des opérateurs pour obtenir le numéro de téléphone à partir de l'identité d'une personne. Ça nécessite pour les flics de vérifier les numéros récupérés par cette méthode (homonymes, faux noms...)
• pour faire de l'identification en masse : les keufs demandent l'identité associée à plusieurs centaines de numéros de téléphones d'un coup, par exemple. Les délais sont de l'ordre de l'heure

En garde à vue / audience / instruction / enquête
Lors d'une garde-à-vue, notre droit au silence est limité par l'« obligation de fournir la convention de chiffrement ». Cette obligation s'applique notamment aux téléphones, si la demande est faite dans son cadre. Dans ce cas, refuser de donner les mots de passe, peut amener en soi un risque de procès. Le cadre permettant qu'une telle demande nous soit faite est le suivant :

• la demande doit être fait par un opj (pas un flic « de base ») supervisé d'un magistrat – procureur ou juge d'instruction.
• elle doit être justifiée, il doit être démontré que le téléphone utilise des méthodes de cryptologie, et que le déverrouillage pourrait permettre d'accéder à des éléments pertinents pour avancer dans l'enquête en cours (« l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit »). S'il ne semble pas y avoir d'enquête approfondi, il ne devrait pas être possible d'y avoir condamnation pour cela.
• il faut qu'il soit démontré que tu connaisses ce code de déverrouillage.
Il reste toujours conseillé d'appliquer les mêmes règles qu'habituellement en garde à vue « je n'ai rien à déclarer » en cas de demande de code de déverrouillage (et pas « je sais pas » ou autre). Ces poursuites ne semblent pas fréquentes, et c'est souvent utilisé comme chef d'inculpation qui en complète d'autres. L'avantage d'exercer ton droit au silence c'est que tu pourras choisir ta défense en cas de poursuite, bien des possibilités peuvent exister.

IMSI-catcher – les fausses antennes relais
Il s'agit d'un dispositif se faisant passer pour une antenne relai officielle, qui capte toutes les connexions téléphoniques dans un rayon défini. Il tiens dans un sac à dos. Sa première fonction est de lister les appareils téléphoniques alentours. Il peut aussi intercepter les contenus en clair tels que les appel et les SMS, mais sert principalement à récupérer les métadonnées : quel téléphone « borne » (est présent dans le rayon défini), quel téléphone appelle quel autre téléphone à quel moment, etc. La police récupère les numéros IMSI et IMEI et peuvent faire des réquisitions auprès des opérateurs pour savoir à qui ça appartient. Il peut aussi voir les sites internet qu'on consulte (mais le https protège ce qui est fait sur les sites que l'on visite).
Un IMSI-catcher ne permet pas de prendre le contrôle d'un téléphone ni d'en extraire les données à distance.
Cependant l'entreprise Nexa a mit au point il y a quelques années un « hacking van ». Grâce à la technologie wifi de Wispear et à un puissant IMSI catcher, la camionnette peut injecter Predator dans les téléphones en mode « zero clic » dans un rayon d'environ 500 mètres[1].

Le Kiosk – extracteur de téléphone
Fabriqué par l'entreprise israélienne « Cellebrite » 500 kiosk ont été achetés et installés dans les comicos. C'est une version tout compris de leur outil « UFED ». C'est un ordi tactile, avec des gros boutons et plein de câbles : il va essayer d'aspirer le contenu du téléphone et de générer des rapports valables aux yeux des magistrats (analyse forensique).
Pour fonctionner, l'UFED exploite des failles de sécurité présentes dans la partie du système d'exploitation qui gère le port USB. L'entreprise promet plein de choses avec cet appareil, notamment le contournement du code de déverrouillage d'écran sur la plupart des téléphones (donc quand le tel est allumé). Elle promet aussi le déchiffrement de nombreux téléphones, en particulier ceux de la marque Samsung. Cependant leur communication est très marketing, et il semble que nombre de leurs promesses ne soient pas réellement applicables.
Ce qui est sûr c'est que l'UFED peut contourner les codes de déverrouillage des téléphones nonchiffrés ou des téléphones chiffrés mais allumés ainsi que cloner la carte SIM.

Boîtes noires
Globalement elles servent à choper à distance la liste des sites internets qu'on visite. Les boites noires font du traitement automatisé de données. Leur réel fonctionnement reste flou, mais elles ne peuvent pas savoir précisément quelles pages on visite lorsque le site est en https (avec le s[écurisé]

1 Voir les Predators Files.

à la fin – la plupart des sites internets). Couplé à d'autres méthodes de surveillance, ça peut permettre de faire des graphes de profilage.

Logiciels d'analyse de données
Les flics utilisent des logiciels d'analyse de données qui leur permettent de faire des graphes de qui parle avec qui. Ils injectent dans le logiciel toutes les informations récoltés principalement dans les communications téléphoniques (que ce soit sur les personnes, lieux, évènements, le matériel).
Ainsi dans les enquêtes sur des militantes, ils essayent de mettre en avant des « organisateurs » de tel mouvement, qui est en contact avec beaucoup de personnes militantes, ou des personnes qui font liens entre plusieurs univers.
Ils peuvent aussi détecter de nouveaux lieux de luttes de manière totalement automatisée. De même ils peuvent détecter les nouvelles militantes via les communications qu'elles ont avec d'anciennes militantes et leur passage dans des lieux de lutte. La surveillance de masse est un enjeu collectif.

A noter que : la grande majorité de la surveillance est automatisée.

Récupération de données en demandant aux propriétaires ou développeurs d'applications ou sites des données qu'ils ont sur vous :
- pour les applications de messagerie, potentiellement l'intégralité de vos messages même ceux supprimés
- pour les applications de type GPS, toutes les adresses que vous avez rentrées dans votre GPS ainsi que l'historique de vos trajets
- pour les applications d'achats, l'historique de vos achats, vos cartes bleues enregistrées, vos recherches,
- pour les navigateurs Web, votre historique de navigation (même s'il est supprimé de votre téléphone si les serveurs de l'application le stockent)
- vos photos, vidéos, etc,
- vos contacts.

Installation de logiciels malveillants[2]
Les technoflics français développent eux-mêmes leurs propres malware (Babar, Bunny, Casper, Tafacalou…)[3]. Et en achètent à des boîtes privées (Predator par ex.). Ils les installent via l'exploitation de failles de sécurité, backdoors, chevaux de Troie ou d'erreurs humaines (voir plus bas social engenieering).
Permet :
- le déclenchement à distance des caméras
- déclenchement à distance micros
- accès à la géolocalisation en temps réel
- captures d'écran à intervalles courts
- enregistrement frappes clavier
- *potentiellement prise de contrôle à distance (reverse shell)*

Certaines des méthodes utilisées par la flicaille ne sont pas encore encadrées par la loi. Les données récupérées illégalement ne peuvent pas être utilisées lors des instructions judiciaires mais peuvent l'être pour mettre la pression afin de récolter des aveux, de faire parler. Il est donc important de ne <u>rien déclarer</u> et ne rien avouer en garde à vue quoi que l'on nous montre ou dise. Il

2 https://blog.ostraca.fr/blog/comment-fonctionne-surveillance-a-distance-des-telephones/
3 https://www.developpez.com/actu/82491/Cyber-espionnage-Apres-Babar-la-France-soupconnee-d-etre-a-l-origine-d-autres-malwares-selon-des-firmes-de-securite/

vaut donc mieux attendre de voir un avocat, des camarades et d'avoir accès au dossier avant de déterminer une stratégie de défense.

Équipes technologiques de la police

Tout au long de ce texte on parle de flics ou de keufs, mais en réalité il existe différents corps au sein de la police et de la justice, qui ont des moyens différents en termes techniques.
La plupart des corps techniques doivent extraire les infos du téléphone sans dégrader celui ci ni laisser de trace de l'intrusion dans le téléphone, c'est ce qu'on appelle « l'analyse forensique ».

Type de parcours possible lors d'une enquête :
Il existe une cellule qui travaille sur une instruction, celle-ci envoie au département informatique-électronique (INL) de l'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) qui a pour mission d'extraire le contenu d'un téléphone et de le ranger dans un disque dur.
Celui-ci peut aussi se déplacer et être présent lors de perquisitions. Il dispose d'enquêteur en technologies numériques (N- Tech), qui sont gendarmes, avec une formation d'officiers de police ainsi qu'une formation dans le domaine informatique de 15 mois à l'UTT de Troyes.

Si cette institution est bloquée par un support chiffré elle peut décider de l'envoyer au CTA (centre technique assistance). Rattaché au ministère de l'Intérieur et aujourd'hui placé sous l'autorité de la DGSI, le CTA est couvert par le secret défense et a le droit d'utiliser des techniques pouvant détruire le matériel à étudier.
Si des informations sont extraites elles sont renvoyées à la cellule d'enquête.

L'IRCGN peut être remplacé par des entreprises d'ingénieur.es agrées sous traitante comme par exemple :
• Tracip : https://www.tracip.fr/
• Informatique legal : https://informatique-legale.com/
• Laboratoire évidences SAS : https://evidences-lab.com/
Plus d'informations sur les équipes techniques:
- "Blog d'un informaticien ancien expert judiciaire" : https://zythom.fr/
- "the french intelligence", compilation de textes sur les renseignements français: https://infokiosques.net/spip.php?article1821

Réduction des risques :

1) Habitudes
Le plan des habitudes est le plus important
* La première habitude à prendre consiste à se poser les bonnes questions. La « modélisation de la menace » est un outil nous permettant de choisir des réponses adaptées à nos besoins.
→ Qui sont nos ennemis potentiels?
→ Que veut-on leur cacher? (liste de contacts, membres d'un groupe signal, contenu de message, localisation, sites web visités, documents enregistrés...)
→ Que risquons-nous si on échoue? (se faire gronder, perdre nos données, prendre une amende, aller en prison...)
→ Quels moyens nos ennemis sont-ils prêts à mettre pour nous ou nos activités? (respect de la loi ou pas, quantité d'argent disponible, protection légale...)
→ Quelle énergie avons-nous à mettre pour nous protéger?

Quelques habitudes à mettre en place :
- Se demander à chaque fois comment faire sans téléphone, si possible (aka «Laisser le tel à la maison»)
- Rendre habituel le mode avion ou éteindre son téléphone quand on a pas besoin du réseau. En mode avion, les téléphones ne communiquent plus avec les antennes et donc il n'y a pas de géolocalisation possible de la part des antennes.

- Stocker le moins de choses possible sur le tel (documents, photos, contacts, messages). Penser à transférer vos données sur un support chiffré (voir partie sauvegarde).
- Dans la mesure du possible, désactivez le stockage de vos données sur le cloud. Vos données ne devraient être stockées que en local et non sur des serveurs distants.
- Effacer son historique régulièrement

- Avoir uniquement des applis qu'on utilise, de préférence opensource et sécurisés. Moins d'applis = moins de failles potentielles. (voir partie apps)
- Sur toutes les applications, mettre les paramètres de confidentialité au maximum afin de limiter les données stockées.

- Lorsque vous ne les utilisez pas, désactiver les services Bluetooth, Wifi et localisation. Il y a parfois des interrupteurs à bascule pour l'appareil photo et le microphone. Les applications ne peuvent pas utiliser les fonctions désactivées (même si elles ont reçu une autorisation individuelle) tant qu'elles ne sont pas réactivées.
- Faire attention au appareils auxquels on se connecte en bluetooth, il est simple de récupérer les contacts, les sms et l'historique d'appels.

- Stickers sur caméra
- Mettre des écouteurs coupés à la sortie jack. On vous conseille quand même de tester par vous même lors d'un appel par exemple. Il est également possible d'enlever les micros (voir partie enlever les micros)
- Gratter les numéros marqués sur le tél (IMEI, à l'intérieur)

- Installer les actualisations dès que possible.
- Redémarrer son téléphone régulièrement. Si il y a une faille exploitée mais pas inscrite dans le téléphone, en redémarrant la faille ne sera plus là.
- Faire un redémarrage d'usine (faire une sauvegarde avant) tous les *x* mois ou quand on pense être infecté. Permet de supprimer toutes les applications (même les malwares)

- Faire de la veille politique et technologique, les téléphones évoluent très rapidement.
- Se former collectivement en cas de garde à vue (« je n'ai rien à déclarer »)

- Jamais prendre son téléphone personnel en manifestation ou en action.
- Supprimer les applications de messagerie en cas de situation à risque.
- Se séparer définitivement de tout téléphone qui a passé un moment dans les mains de la police loin de votre surveillance. (Ou a minima faire un redémarrage d'usine)

- Face aux écoutes, choisissez bien vos sujets de discussion par téléphone. N'hésitez pas à couper votre interlocuteur si il parle d'un sujet sensible par téléphone. Cela n'est absolument pas le bon moyen de communication pour ce genre de discussions. Les SMS et appels ne sont pas chiffrés et donc visibles par l'opérateur ainsi que par la police en cas de mise sur écoute.
Il est important de noter que les écoutes sont enregistrées numériquement, stockées et peuvent resservir des années plus tard lors d'une enquête.

- Compartimenter. Créer plusieurs profils ou avoir des téléphones différents pour des usages différents.
- Il est aussi possible ça soit pris en charge collectivement : que le collectif fournisse des téléphones anonymes pour une tache spécifiques dans la lutte. (voir téléphone anonyme)

- Privilégier Tails (voir plus bas)

Note sur éteindre son téléphone :
Il est possible qu'un spyware arrive à simuler un état éteint sans l'être réellement. Pour être sur que son tel est éteint : - enlever la batterie
- iphone : entrer en mode DFU (device firmware upgrade) > voir instructions sur internet.
- android : entrer en mode fastboot : éteindre le tel puis maintenir le bouton *allumage* et *volume bas*

2) Modifier les réglages du téléphone
* Mode USB par défaut : charge uniquement
* Débogage USB désactivé
* Chiffrement du téléphone (il est activé par défaut depuis android 10)
* Mettre un verrouillage d'écran rapide + un bon code de déverrouillage (voir partie mot de passe)
* Désactiver l'identifiant de publicité ciblée qui récolte des données personnelles soit dans Paramètres → Google → Annonces soit dans Paramètres → Confidentialité → Publicités
* Notifications discrètes (que le téléphone n'affiche pas le contenu du message)
* Utiliser les Comptes d'Utilisateurs pour séparer certains usages, ou une application d'isolement d'applis telle que Insular ou Shelter (voir partie compartimentation)
* ***Désactiver les sauvegardes sur cloud*** (Cloud open bar pour les agences étatiques)
* Vérifier adresse mac aléatoire (activé par défaut normalement)

3) Les réseaux sociaux
La quantité d'informations qu'on peut donner sur soi-même sur un réseau social est considérable. Utiliser un compte sur un réseau social pour consulter des informations militantes, c'est offrir à la police et aux géants du Web (Facebook, Twitter, Instagram, etc.) des données que l'on souhaiterai probablement garder cachées.

- Quitter les réseaux sociaux.
- Sinon de créer des comptes anonymes. (voir partie sur l'anonymat)

- Si vous aimez quand même le concept des réseaux sociaux par exemple pour rester en contact avec des amies, le réseau Mastodon est plus respectueux de la vie privée.
- Vous pouvez aussi choisir de ne plus poster sur les réseaux sociaux tout en gardant votre compte et en augmentant aux max les paramètres de confidentialité (compte privée…) et ne pas donner des infos personnelles.
- Ne pas mettre son nom + prénom complique un peu la surveillance.
- Si vous utilisez les réseaux sociaux pour vous informer, on vous pouvez utiliser les flux RSS5. S'abonner au flux RSS d'un site, c'est comme lui demander de nous envoyer le nouveau contenu, au fur et à mesure qu'il est publié.

La protection de la vie privée dépends de votre attitudes, des infos que vous y stockez et des apps utilisées

4) Applis libres
Les applications ont un grand pouvoir de surveillance. C'est pourquoi on peut choisir d'utiliser des applications « de confiance ».
La confiance en une appli peut se jouer à différents endroits:
- sécurité "l'appli fait-elle bien ce qu'elle dit et dit-elle bien ce qu'elle fait"
- fiabilité dans le temps : Est-ce que les gens continuent de travailler dessus pour corriger les vulnérabilités ?
- Vérifier réputation des gens qui font le logiciel.
- Tchéquer le modèle économique du logiciel.

Une tendance lorsqu'on parle de sécurité est d'utiliser des logiciels libres. Avec une appli privative, on ne pourra pas vérifier profondément la qualité de l'appli en terme de sécurité. Une appli libre permettra à une communauté de scruter son fonctionnement et avec un peu de chance de reprendre le développement si l'équipe d'origine quitte.
Une appli non-libre pourrait volontairement chercher à nuire (de manière large ou de manière ciblée), sans qu'on puisse s'en apercevoir sans l'installer, car sa recette n'est pas rendue publique.

/!\ Attention, libre ≠ sécure, une appli libre peut contenir du code malveillant (volontairement ou non).
De plus, certaines applications ont une réputation, basée sur plusieurs éléments:
- la qualité de l'application dans le temps
- la réactivité à la correction des vulnérabilités
- la réputation de l'équipe de développement
- le modèle économique
- les phénomènes de mode
Enfin, il est important de bien toujours **mettre à jour** ses applis, afin de profiter des corrections de sécurité.

Magasin d'applications :
* F-Droid (ne propose que des applis libres) f-droid.org
* Aurora Store (à installer depuis f-droid) (interface libre à Google Play Store, permettant de l'utiliser sans compte google et qui ne transmet pas à google tout un tas d'infos quand on installe une app) (rappel : les applis dans le Play Store sont pour la plupart non-libres et peuvent potentiellement être modifiées par google).
(Si les recherches sont limités sur Aurora Store : Paramètres->Apps->Aurora Store->Ouvrir par défaut/Ajouter un lien. Activez ensuite ces cases à cocher. Aurora devrait alors se lancer si vous cliquez sur un lien Play Store dans un navigateur.)

Applis open source :
La série d'applis Simple Mobile Tools n'est plus du tout conseillée depuis son rachat par ZipoApps[4] fin 2023.

Clavier : * FlorisBoard – la confiance dans le clavier est super important !

Applis de sécurité : * exodus : εxodus analyse les applications Android dans le but de lister les pisteurs embarqués.
* Hypatia : Scanner de malware, fonctionne hors internet.
* Appli SnoopSnitch : SnoopSnitch analyse le micrologiciel de votre téléphone à la recherche de correctifs de sécurité Android installés ou manquants. (Pour les android « rooté » ce logiciel pourrait permettre de détecter les IMSI catcher.)
* Netguard : pare-feu

Photos: * Open Camera
* Obscuracam : qui peut être configuré pour flouter les visages automatiquement.
* Signal (prendre direct dessus les photos que vous voulez envoyés). Pas de métadonnées. Possibilité de flouter.

Vidéos : * VLC

Lecture de documents : * Librera (pour lire des ebooks)
* MuPDF (pour afficher PDF et autres)
* Document Viewer (pour afficher PDF et autres)

Audio/visio-conférence : * Signal
* Jitsi (audio/vidéo à plusieurs)

Calendrier/agenda : * Etar (fonctionne hors-ligne)
* DAVx (synchronisation de calendrier distant, avec Nextcloud par exemple)

Notes : * Notepad

Lecteur Youtube/Bandcamp/Soundcloud/Framatube : * NewPipe (permet de télécharger videos en mp3 ou mp4!)
Reddit browser : infinity
Twitter browser : nitter

Cartes : * OsmAnd (basé sur Openstreepmap)
* Organic Maps (idem)

Cloud : * NextCloud

Effacement données d'urgence (à tester) : *Wasted
* Riple

5) Applis visant à protéger la confidentialité des communications :
Un système de chiffrement dit bout-à-bout est un système qui chiffre les communications de manière à ce que seuls le destinataire et l'expéditeur puisse déchiffrer.

- Signal (protocole de chiffrement Signal, compte relié à un numéro de téléphone)
- Briar (protocole de chiffrement Briar, compte pas relié à un téléphone, utilise Tor si on veut, fonctionne aussi sans internet via Bluetooth.

4 https://www.androidauthority.com/simple-mobile-tools-acquisition-3391041/

- Conversations (protocole de chiffrement XMPP/Jabber, d'origine pour ordi, l'appli Android est finalement carrément mieux que ses équivalents ordi)
- Element (protocole de chiffrement Matrix, compte pas relié à un téléphone)
- Silence (protocole de chiffrement pour les SMS – attention, les contacts restent visible sur le réseau contrairement aux autres logiciels)

Un certain nombre d'applis ont des versions ordinateurs – à prendre en considération pour avoir des communications ordi-téléphones : Signal (Signal-desktop, axolotl.chat), Conversations (Dino, Pidgin, Gajim, ...), Element

Revenons sur les applis de chiffrement bout à bout les plus répendues :
WhatsApp (pas dispo sur f-droid)
- Données liées à vous
- Non open source, sauf pour le cryptage (Signal Protocol)
- collecte énormément de données perso (emplacement géographique, historiques d'achat, numéro de téléphone, contacts, fréquence d'interaction, etc.).
- Donne les données perso, carnet d'adresse, contacts en cas d'enquête. Il est possible de collecter en temps réel les métadonnées des messages (« Pen registrer »).
- Le contenu des messages peut-être récupéré par l'intermédiaire de sauvegardes Cloud (à désactiver).
- Impératif de désactiver le « téléchargement automatique des médias »

Telegram
+ dispo sur f-droid et sur tails (Telegram-FOSS)
- données liées à vous (nom, numero de téléphone, contacts, ID utilisateurs)
- chiffrement partiellement open source
- Messages cryptés à activer pour chaque conversation
- Conversations de groupe ne peuvent pas être cryptés
- collecte ip
- Donne adresse ip et numero de téléphone en cas d'enquête sur des « terroristes »

Revenons sur Signal
Signal est disponible depuis aurorastore ou en apk sur leur site.
Molly est une fork de signal disponible sur f-droid qui a pour but d'augmenter la sécurité. Le dépôt s'ajoute sur f-droid depuis leur site molly.im. L'utiliser oblige à faire confiance aux développeurs de Molly en plus de ceux de signal, un débat existe donc sur l'augmentation réelle de sécurité.

Défauts :
- Lié à un numéro de téléphone. On peut désormais le cacher et partager un nom d'utilisateur à la place !
- Possible sensation de sécurité parfaite (illusoire) qui fait qu'on ne fait plus attention à ce qu'on envoie
Poinsts forts :
- Ne collecte pas les données. En cas de réquisition judiciaire faite à Signal, Signal dit ne posséder que la date de création du compte ainsi que la date de la dernière connexion au compte.
- Chiffrement bout à bout Signal Protocol (chiffrement qui a été repris par whatsapp, messenger google allo - mais ces dernières collaborent avec les agences gouvernementales -)
- À aucun moment Cellebrite (voir plus haut -le kiosk) n'a créé un outil capable de pénétrer Signal, et elle n'a certainement pas cassé le chiffrement de l'app.
- Possible de flouter les visages

Options sur Signal pour renforcer la sécurité :
- Ne pas gérer les SMS/MMS et utiliser une appli dédiée (silence par ex. pour ne pas se mélanger les pinceaux)
- Nom, À propos, Photo donner le minimum d'informations
- Mettre un NIP (/!\ ) et activer blocage d'inscription (compte) (évite simswap)
- Vérifier les appareils reliés régulièrement. (linked devices)
- Option "Aperçus de liens" à désactiver (chats)
- Option "Toujours relayer les appels" à activer (ça permet de ne pas divulguer l'adresse IP de notre connexion aux destinataires de nos appels) (privacy -advanced)
- Option "Clavier incognito" à activer (privacy)
- Activer les messages éphémères et mettre une valeur par défaut (privacy)
- Option sealed sender à activer (privacy -advanced) (réduit les metadonnées entre nouveaux contacts)
- Verrou d'écran à activer sur le smartphone (privacy)
- Sécurité de l'écran à activer (privacy)
- S'assurer que les notifications n'affichent rien si le téléphone est verrouillé. (notifications)
- Numéro de sécurité à vérifier avec ses correspondantes
- On peut modifier l'apparence de l'appli (appearance)

6) Mail

La plupart des clients mails utilisent le protocole TLS qui est un système de chiffrement. Ce protocole chiffre la communication entre les serveurs mails.
Cependant les serveurs de mails ont accès aux communications et peuvent les lire. Par exemple, si vous utilisez un compte Gmail, Google lit vos communications et récupère les données. Il le fait de manière automatique pour récupérer vos infos perso et les revendre. La plupart des mails collaborent avec les institutions gouvernementales.

Pour mieux vous protéger, y compris de vos hébergeurs d'adresse mails, on vous conseille d'utiliser le protocole PGP qui est un mécanisme de chiffrement bout-à-bout que vous contrôlez. Vous n'aurez de plus plus à faire confiance aux acteurs intermédiaires pour bien chiffrer vos données vu que vous le ferez vous-mêmes.
Faites attention également aux usurpations d'identité. Le système PGP vous protège de ces usurpations via un système de signature numérique.
Thunderbird ou Kleopatra (installé sur tails) facilitent l'utilisation de clefs PGP.
Pour en savoir plus sur le protocole PGP et comment s'en servir nous vous conseillons la partie « Cacher le contenu des communications : la cryptographie asymétrique » du « guide d'autodéfense numérique ».

A défaut de gérer les clefs soi-même, certains clients mail gèrent automatiquement le chiffrement bout à bout entre 2 utilisateurs du même service. Entre différents services, le chiffrement est TLS. Ces clients mails chiffrent bout à bout le contenu de votre boîte mail sur leurs serveurs (vous êtes les seuls à posséder les clefs de déchiffrement) :
- Riseup : Ne chiffre pas l'objet du mail (conseil : le laisser vide). A collaboré en 2017 avec le fbi sur 2 mandats[5]. Depuis les serveurs sont chiffrés et vous êtes les seuls à disposer des clefs de déchiffrement. Ne garde pas les logs de connexion.
- Protonmail : Ne chiffre pas l'objet du mail (le laisser vide). Option d'envoyer un message chiffré à n'importe qui avec un mot de passe. Permet utiliser PGP avec d'autres clients mails facilement.

5 https://riseup.net/en/about-us/press/canary-statement

Protonmail a collaboré dans le cadre d'enquêtes[6] : ils sont en capacité de révéler l'adresse IP d'un compte mais rien d'autre (ne détiennent pas vos clefs de chiffrement). (utiliser tor ou VPN)
- Tutanota (appli dispo sur f-droid) : Chiffrement mail différent que PGP, résistera aux ordinateurs quantiques selon eux. Chiffre l'entête. Option d'envoyer un message chiffré à n'importe qui avec un mot de passe. Tutanota a collaboré dans le cadre d'enquêtes[7] : ils ont donné accès aux mails qui n'étaient pas chiffrés bout à bout (tls) mais rien d'autre (ne détiennent pas vos clefs de chiffrement).

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

Le client mail *Thunderbird (K9* sur smartphone) permet de centraliser sur une même application plusieurs adresses mails. On conseille de les utiliser uniquement si le disque dur de l'ordinateur est chiffré car sinon toute personne ayant accès à votre ordinateur pourra lire vos mails. Il faudra préférer consulter ses adresses mails sur un onglet privé d'un navigateur (Tor Browser de préférence) si le disque dur n'est pas chiffré.

Simplelogin – permet de créer des alias gratuitement. Racheté récemment par proton. Site web et appli sur f-droid.

Changer d'adresse mail :
- Faire une sauvegarde de ses mails : exporter les mails dans un fichier puis ouvrir ce fichier avec un nouveau client mail. (en profiter pour faire le ménage)
- Changer le mail pour chaque compte. Utiliser des alias pour réduire les spam et protéger votre mail. (Simplelogin)
- à chaque fois qu'un mail arrive sur « l'ancienne boîte », le transférer et changer le mail.
- attendre quelques semaines jusqu'à ce qu'aucun mail n'arrive sur « l'ancienne » boîte mail puis fermer son compte
- proton mail facilite la migration depuis des comptes google

7) NAVIGATION WEB

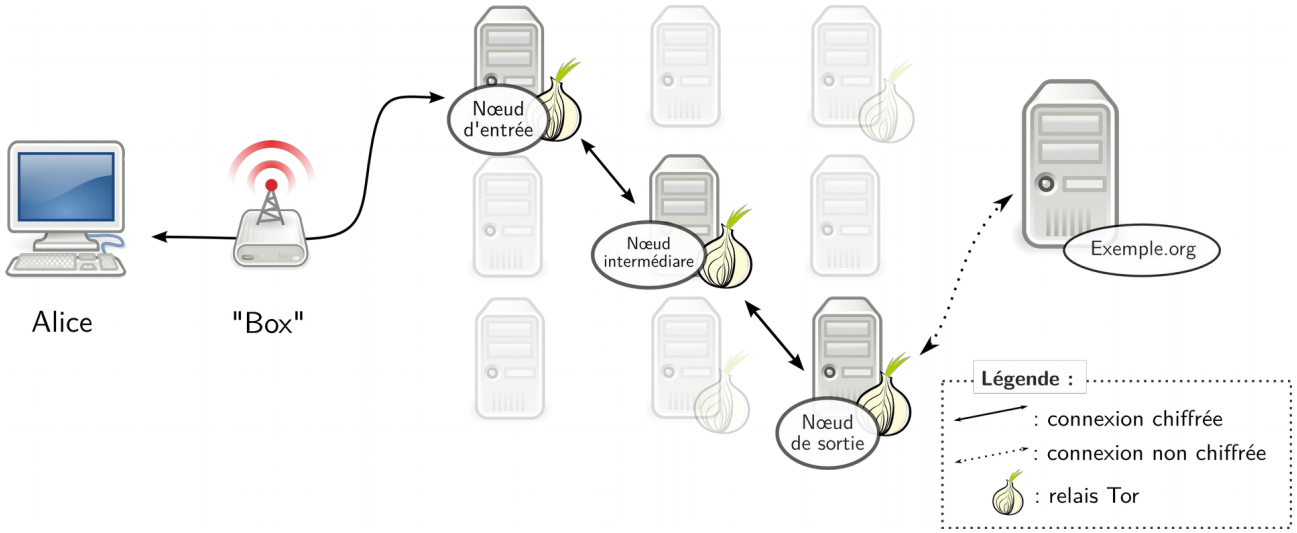
Quand vous naviguez sur le Web, vous demandez à votre fournisseur d'accès Internet de communiquer avec les serveurs qui gèrent les sites Web que vous visitez. Ce dernier peut donc savoir quels sites vous consultez. Votre activité sur le site n'est pas accessible si le site est en https. Les autorités peuvent demander à votre fournisseur d'accès Internet l'historique de votre utilisation d'Internet.

TOR

Pour se protéger face à cette attaque, on conseille d'utiliser Tor. Tor fait en sorte qu'aucun serveur ne sache avec qui vous souhaitez communiquer en utilisant 3 nœuds qui n'ont accès qu'à des informations partielles. Le premier nœud connaît l'émetteur et le premier nœud intermédiaire.
Le nœud intermédiaires ne connaissent que le nœud précédent et celui suivant. Le nœud de sortie connaît le nœud intermédiaire et le serveur destinataire.
Votre trafic est relayé et chiffré trois fois alors qu'il traverse le réseau Tor. Le réseau comprend des milliers de serveurs gérés par des bénévoles, appelés relais Tor.

6 https://www.theverge.com/2021/9/6/22659861/protonmail-swiss-court-order-french-climate-activist-arrest-identification

7 https://www.internetsociety.org/blog/2021/03/enough-is-enough-what-happens-when-law-enforcement-bends-laws-to-access-data/



Le Navigateur Tor isole chaque site Web que vous visitez afin que les traqueurs tiers et les publicités ne puissent pas vous suivre. Tous les témoins sont automatiquement effacés une fois la navigation terminée. Il en sera de même pour votre historique de navigation.

Le Navigateur Tor vise à rendre tous les utilisateurs semblables en apparence, afin qu'il soit plus difficile de vous suivre d'après l'empreinte numérique unique de votre navigateur et les renseignements de votre appareil

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

Configuration tor et usage :
- Général – Mises à jour : comme pour tout logiciel, il est toujours préférable de le maintenir à jour. Voilà pourquoi l'option « Mise à jour automatique » doit être sélectionnée.
- Vie privée et sécurité – Historique – Mode de navigation privé permanent : cette option est similaire à celle qui consiste à toujours ouvrir le navigateur en mode « incognito », c'est-à-dire qu'elle ne sauvegarde jamais l'historique de la navigation, les cookies ou tout autre fichier ou trace des sites visités.
- Vie privée et sécurité – Autorisations : Il est préférable de ne pas accorder les autorisations aux sites que nous visitons, l'accès à l'emplacement, à la caméra, au microphone et aux autres dispositifs de votre ordinateur.
- Vie privée et sécurité – Sécurité : Il est préférable de mettre le navigateur en mode « Plus sûr », ce qui empêche l'exécution de certains JavaScripts, de certaines polices et symboles et surtout l'exécution automatique de fichiers audio, vidéo et autres fichiers multimédia.
- Vie privée et sécurité – Services Onion : Certains sites proposent des urls en .onion. Ainsi la connexion reste sur le réseau tor et reste chiffré tout du long
- Vie privée et sécurité – Mode https uniquement

Extension à installer : UblockOrigin (bloque les pubs et certains malwares, augmente la vitesse de chargement des pages) (préinstallé sur tails)

Prenez soin de ne pas mélanger vos identités sur un même navigateur sur le même circuit tor. Pour changer de circuit tor, allez dans le menu latéral e haut à droite puis cliquez sur « nouvelle identité ».

Il est important de noter que la navigation Web n'est pas le seul moment où vous utilisez Internet depuis un ordinateur. En utilisant Tor Browser par exemple, vous ne protégez votre IP que pendant votre navigation mais pas le reste du temps.
Lorsque vous utilisez tor, n'utilisez pas un autre navigateur en parallèle.
Le système d'exploitation Tails (voir plus bas) est pensé pour que absolument toutes les connexions à Internet passent par Tor.

Ponts
Tor et certains vpn vous permettent d'utiliser des ponts. Les ponts sont des serveurs tor ou vpn secrets. Votre fournisseur d'accès internet aura plus de mal à déterminer l'utilisation de tor ou vpn. Aussi les sites que vous visitez vous bloqueront moins l'accès.

Pour réduire la censure, il est aussi possible de changer de circuit tor ou de serveur vpn.

VPN
À défaut d'utiliser Tor, vous pouvez utiliser un VPN. Vous n'avez plus qu'un acteur intermédiaire entre vous et le serveur final.

Ordinateur – « boxe » – serveur vpn – serveur

Cet intermédiaire a donc accès aux sites que vous visitez contrairement à Tor.
Cependant votre fournisseur d'accès Internet sait juste que vous souhaitez communiquer avec le serveur de votre VPN et le trafic est chiffré.

Listes des vpn conseillés :
- RiseupVPN (gratuit, pas de logs)
- Mullvad VPN (payant mais possibilité de payer en cryptomonnaies, pas de logs)
- CalyxVPN (gratuit, pas de logs)
- Proton VPN (gratuit, création de compte à réaliser depuis tor avec un mail anonyme)

A partir de Android 7, possibilité d'activer l'option vpn permanent et le filtrage des connexions sans appli tierce (paramètres – réseau et internet – vpn / ou via les réglages de l'appli). Permet de bloquer les connexions a internet quand le vpn n'est pas en place.

Il est possible d'activer le mode avion, puis d'activer le wifi et un vpn ou tor.

Le navigateur
Le choix du navigateur est important pour préservez vos informations personnelles et participe à votre sécurité. Nous vous conseillons de supprimer ou désactiver si pas possible :
- Chrome, Edgde, Safari, google (sur smartphone)
A la place privilégiez un navigateur open-source sécurisé et qui a pour objectif de protéger la vie privée de ses utilisateurs :
- Brave (ordi, mobile) Bloquer de pubs et trackers intégré
- LibreWolf. (uniquement ordi) Version modifié de Firefox destinée à augmenter la protection contre le tracking tout en ajoutant des améliorations sur la sécurité.
- Firefox focus (dispo uniquement sur tel)
- Duckduck go (dispo uniquement sur tel)

Paramètres :
Voir paramètres Tor (plus haut)

Si vous souhaitez activer javascript pour des sites de confiance, nous vous conseillons d'utiliser 2 navigateurs. Un qui ouvre les liens par défaut, avec les paramètres de sécu au max et un second avec javascript activé.

Extensions conseillées
Ublock origin
Privacy Badger
Https everywhere

Moteurs de recherche conseillés sans trackers qui respectent votre vie privée :
- Brave
- Duckduckgo

8) Anonymat téléphone
Carte SIM « anonyme »
Des solutions partielles comme les cartes SIM prépayées peuvent considérablement compliquer le travail de la justice. Même si les services de renseignement arrivent à relier votre numéro à votre identité, ils devront encore le prouver aux juges.

Il existe plusieurs marques de sim prépayées : SFR, Lycamobile, Lebara, Syma (d'autres opérateurs en proposent, à tester).
- Récupérer une nouvelle carte SIM dans un bureau de tabac et payer en liquide ton crédit qui permet de remplir le téléphone. En cas de recherche la police peut savoir dans quel bureau de tabac a été acheté le forfait. Le lieu de vente de la carte SIM peut être équipé de vidéosurveillance, les enquêteurs peuvent vous identifier à partir des images.
- Certaines marques demandent d'activer la carte SIM. Des données personnelles sont demandées mais on peux donner des informations imaginaires voir fantaisiste, il n'y a pas de vérifications. Parfois il faut un peu de temps (quelques heures) avant que ça soit effectif, c'est bien de préparer le téléphone à l'avance. Il faut ensuite activer le crédit.
- Syma, par exemple, ne nécessite pas d'activation pendant 30 jours.

A noter que :
- L'opérateur conserve l'historique du bornage (borner chez vous compromet l'anonymat)
- Si vous mettez une carte SIM prépayée avec une fausse identité dans un téléphone
que vous utilisiez auparavant, le numéro IMEI du téléphone reste le même. Cela permet d'établir un lien.
- Si vous achetez un téléphone neuf avec un moyen de paiement nominatif, le numéro IMEI du téléphone pourra aussi être relié à votre identité.
- Pour compliquer la tâche des autorités, utilisez un téléphone acheté cash où vous n'avez jamais mis de cartes SIM à votre nom.
- Les recherches premières des flics se limiteront à faire une requête aux opérateurs pour connaître l'identité des personnes derrière un numéro IMSI ou IMEI. Ils peuvent mettre en place d'autres méthodes pour savoir qui est derrière un téléphone (mise sous écoute, étude des numéros contactés avec le téléphone, etc), ou peuvent mettre sous écoute tes proches pour trouver ton nouveau numéro lorsque tu les appelleras. Mais ça demande plus de moyens.

Avoir un téléphone sans carte sim
Il est possible de ne pas utiliser du tout le réseau mobile. Ne pas mettre de carte sim dans son téléphone, le laisser en mode avion (tout le temps!) et activer le vpn permanent est une bonne façon de réduire la surface d'attaque et d'augmenter l'anonymat.

Comptes anonymes
Pour créer des comptes, il est souvent nécessaire d'avoir un numéro de téléphone.
- sim prepayée (voir plus haut)
- Il est existe des téléphones à boutons avec carte sim prépayée crédit dispo desuite (20€), pas besoin de s'enregistrer. Permet de ne pas révéler son IMEI et rester en mode avion sur le smartphone où on veux un code de vérif. (penser à ne pas borner chez soi)
- Enfin certains sites internet proposent de recevoir en ligne des sms gratuitement. Il proposent plusieurs numéros de téléphone. Il suffit de mettre un de ces numéros pour l'enregistrement d'un compte souhaité. Tous les sms que reçoit ce numéro sont visibles. (par ex : receive-sms-free.cc)
Pensez à activer un mfa (voir partie mots de passe), pour éviter le simswap (la carte sim est clonable)
Pour éviter le ban ou le shadowban des comptes sociaux : avoir un mail et un numéro de téléphone associés au compte. Faire du follow sur follow sans en abuser un peu tous les jours pour faire grossir le compte. Poster des publications régulières. Avoir une photo de profil. Faire des publications régulières. Prenez des vraies photos, de d'autres photos ou de dessins (des algorithmes repèrent les métadonnées et l'ia reconnaît les photos).

Navigation gps
vous pouvez mettre votre téléphone en mode avion puis activer le GPS sur une carte téléchargée. Vous évitez ainsi d'être géolocalisé par votre opérateur. Le gps ne connaît pas votre position, c'est vous qui connaissez la sienne. Par contre votre appli de carte peut collecter vos recherches, utilisez une carte opensource qui ne collecte pas d'info (omsand). Si vous activez le gps d'autres applis peuvent y avoir accès, préférez donc un autre profil où il n'y aura que l'application de carte.

N'oubliez pas de créer vos comptes via tor ou un vpn de confiance activée ainsi que de vous connecter à vos comptes de via tor ou vpn pour ne pas révéler votre adresse ip perso. 1 seule connexion sans vpn suffit pour compromettre votre anonymat.

9) Mots de passe
Les dangers : réutilisation des mêmes mots de passe et mots de passe courts

Plus un mot de passe est utilisé, plus sa sécurité baisse.
Si le site ou app à qui vous avez donné ce mot de passe se font attaquer, les attaquants peuvent récupérer votre identifiant et votre mot de passe et l'essayer sur d'autres services où vous avez donné un mot de passe.
haveibeenpwned.com recense des fuites de sécurité et vous dit si un mot de passe lié à votre adresse mail a pu fuiter lors d'une attaque informatique. (dans ce cas changer de mdp)

Une autre erreur concernant les mots de passe est leur robustesse trop faible. Un mot de passe trop court pourra être trouvé par force brute. La robustesse d'un mot de passe dépend de sa longueur, l'utilisation de caractères spéciaux (majuscules, chiffres, etc.) et son caractère aléatoire (il existe des dictionnaires de mots de passe qui recensent les mdp les plus fréquents). Les meilleurs mots de passe sont souvent ceux générés aléatoirement et qui comportent au moins 16 caractères. Les gestionnaires de mots de passe (voir plus bas) proposent ce genre de fonctionnalités.

Une méthode facile pour retenir des mots de passe est de retenir une phrase. On peut aussi souhaiter améliorer la robustesse de la phrase de passe en modifiant légèrement les mots du dictionnaires ou en ajoutant des caractères spéciaux entres les mots ainsi qu'ajouter des chiffres. Ici la taille compte, long c'est toujours mieux.

Les gestionnaires de mots de passe permettent de se simplifier la vie.
Pour éviter d'utiliser plusieurs fois le même mot de passe et avoir des mots de passe longs, on conseille d'utiliser un gestionnaire de mot de passe et d'utiliser au maximum des mots de passe à usage unique.
KeepassXC (KeepassDx sur smartphone) est un gestionnaire de mot de passe sécurisé et opensource. Cette application peut stocker dans une base de données un grand nombre de mots de passe. Idéalement le mot de passe principal qui débloque la base de mots de passe doit être long et unique à cette base de données. Cela permet de ne pas avoir à se souvenir de tout les mots de passe à usage unique que vous utilisez, mais uniquement de celui qui permet de débloquer la base de données. (penser à faire des sauvegardes – voir plus bas)
Sur smartphone, il y a l'option « clavier magique » qui vous évite de faire des copie-collés des mdp (visibles par les autres apps)
Pour en savoir plus sur l'utilisation de keepass, rdv sur le site de surveillance self-défense : https://ssd.eff.org/fr/module/guide-pratique-utiliser-keepassxc

Multiple Factor Authentication (MFA) ou vérification à 2 étapes (2FA)
Un facteur d'authentification est une façon de vérifier que c'est bien vous qui vous connectez. Les 3 principaux facteurs sont :
- Quelque chose que l'on connaît : mot de passe
- Quelque chose que l'on a : smartphone (accès à ses sms, mail, application), clef usb sécurisée (ubkey).
- Quelque chose que l'on est : empreinte, reconnaissance faciale
Il n'est pas de trop d'activer systématiquement plusieurs facteurs d'authentification sur ses comptes.
Aegis Authenticator est une application opensource sécurisée (dispo f-droid et ggplaystore) qui permet de générer un code de vérification.

Pour le smartphone :
Le code de chiffrement est le même que le code de déverrouillage de l'écran.

- Éviter la reconnaissance faciale (problématique en tant que technologie et y a des failles) et empreinte digitale (c'est possible de forcer la personne à mettre son doigt).
- Les schémas, souvent il reste des traces sur l'écran qui permet de les refaire.
- Digicode: bien à condition d'en avoir un assez long. C'est encore mieux si on active l'option "disposition aléatoire" disponible sur certains systèmes.
- Phrase de passe: le mieux en terme de sécurité.

Penser à éteindre un appareil chiffré avant saisi pour activer le chiffrement.
Il existe des options qui permettent de redémarrer le smartphone à une heure précise automatiquement.

10) Les métadonnées des fichiers
Les photos, fichiers PDF ou textes peuvent contenir des métadonnées qui renseignent sur l'heure de dernière modification, la marque de l'appareil photo (pour les photos), la localisation, etc.

On conseille de les supprimer systématiquement dès que l'on partage un fichier. Le système d'exploitation Tails intègre le logiciel mat2 pour supprimer les métadonnées (click droit sur fichier – effacer métadonnées).
Sur smartphone ScrambleExif

11) Compartimentation

Compartimenter permet de « ne pas mettre tous ses œufs dans le même panier ». Compartimenter permet de séparer les usages, ne pas mélanger ses identités et ne pas « tout perdre » si un compartiment en compromis. Il convient alors de préciser les besoins respectifs, en matière de confidentialité, de ces diverses activités et à partir de là, de faire le tri et décider lesquelles, plus « sensibles » que les autres, doivent bénéficier d'un traitement de faveur.

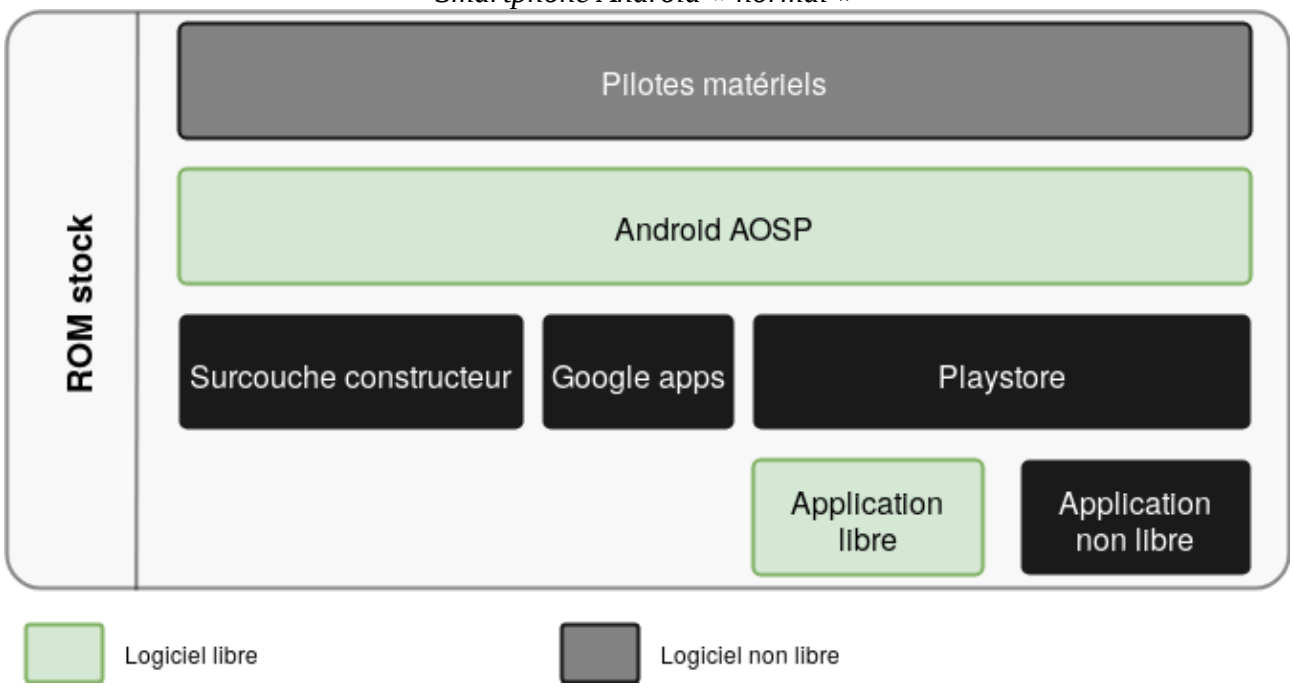
Exemples de compartimentation :

- Utiliser plusieurs os sur ordinateurs (voir tails).
- Utiliser plusieurs téléphones (voir plus bas).
- Avoir 2 mails différents : un perso et un autre pour s'organiser politiquement. Créer et se connecter que par tor ou via un vpn pour que le mail ne soit pas relié à notre identité.
- Utiliser différents profiles. Sur smartphone comme sur ordi, utiliser différents profiles permet d'isoler des applications. Les applis sur différents profiles ne communiquent pas entre elles. On conseil d'utiliser le moins possible son profil administrateur et de privilégier des utilisateurs invités. Une appli malveillante devra escalader plus de privilèges.
- Sur smartphone, des applis permettent d'isoler des applis au sein d'un même profil : Insular ou Shelter.

Pensez à activer le vpn pour chaque profil

12) Changer de système d'exploitation (OS) sur smartphone :

Smartphone Android « normal »

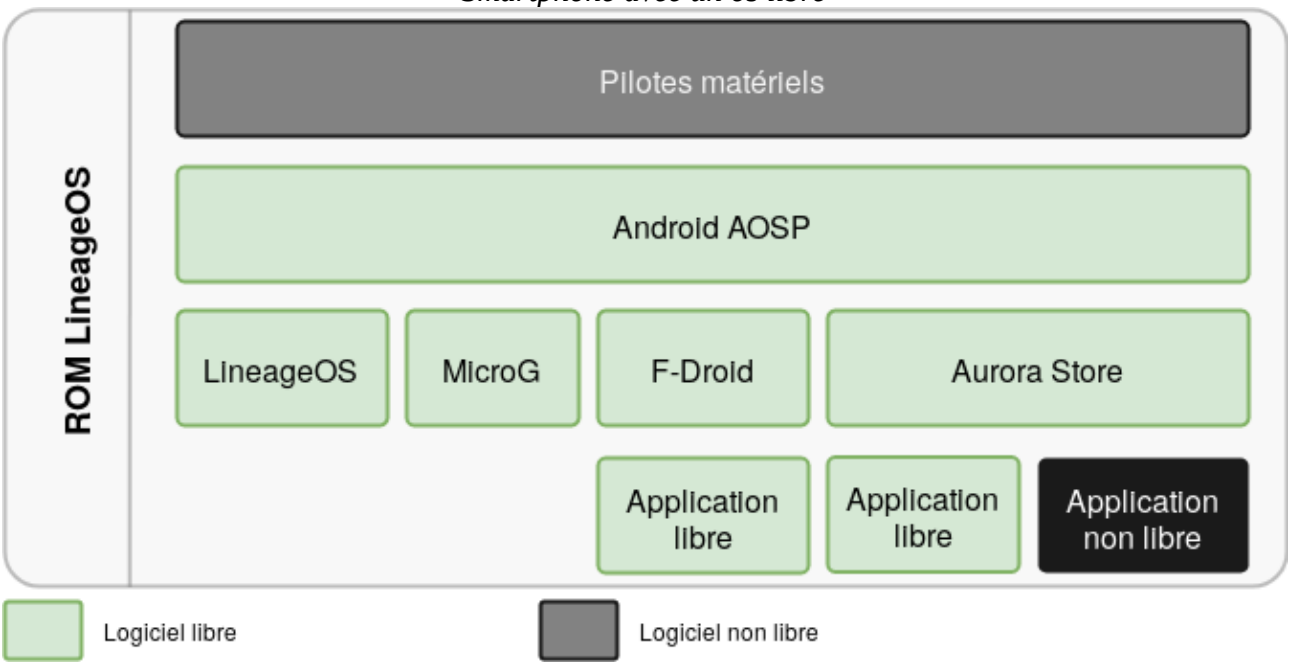


- La base Android (AOSP) est libre, mais le reste qui est dedans ne l'est pas.
- Par dessus ça les fabricants de téléphones (Samsung, Xiaomi...) prennent android plus les logiciels google et ajoutent leurs merdes (samsung quies, MiUI, …)
- Il y a des morceaux de logiciels des fabricants de composants (souvent propriétaires), comme les pilotes wifi ou d'autres trucs.
- Les opérateurs téléphoniques rajoutent aussi parfois des trucs, comme Orange Music ou autres.

Si un des acteurs ne fournit pas les mises à jour, c'est pas possible de faire la mise à jour sur le smartphone. Beaucoup de téléphones sous Android n'ont plus de mises à jour rapidement après leur lancement. Cela signifie que les failles de sécurité découvertes dans le temps ne sont pas corrigées.

De plus chacun de ses acteurs laisses des portes dérobés (backdoors) pour les agences gouvernementales.

Smartphone avec un os libre



Installer un OS opensource permet de réduire grandement la surface d'attaques (0 backdoors intentionnelles). Pas de surcouche constructeur (gagner en sécurité, vitesse d'exécution et en espace libre).
Nécessite d'avoir un téléphone compatible (liste disponible sur les sites respectifs des systèmes d'exploitation)
Systèmes d'exploitation libres :

- GrapheneOS – Uniquement sur les google pixel 6a et + (occasions autour de 200€ juin 2023). **Le top niveau sécurité**, implémente plusieurs paramètres de sécurité en plus et réduit grandement la surface d'attaque. Permet par exemple de faire un autoreboot au bout de x minutes sans déverrouillé le tel.
Pour comprendre pourquoi graphene et pourquoi graphene utilise les google pixel on vous conseille une video de The hated one : « Here's How They Built The Most Secure Phone On The Planet ».
Pour faire simple, l'intêret des pixel est la confiance que l'on peut porter dans le hardware et en particulier la puce de sécurité titan M.
Graphene est aussi le plus simple à installer. En effet, depuis leur site, ils proposent un web installer.
Si vous cherchez à changer de tel, prenez un pixel !

- LineageOS – Large catalogue de tels compatibles. Un très bon tutoriel explicatif de pourquoi et comment installer LineageOS sur smartphone est disponible à cette page : https://linuxfr.org/news/installer-lineageos-sur-son-appareil-android
- DivestOS Mobile – Se base sur lineageos avec pour but d'augmenter la sécurité.
- /e/OS – Se base sur lineageos avec pour but de faciliter l'utilisation. Contient des logiciels propriétaires.
- ReplicantOS – à pour but de construire une version d'Android entièrement libre (y compris les pilotes)
- Il existe un téléphone vendu avec un système d'exploitation libre:
Murena, sur https://murena.com, à partir de 330€.

- Smartphone totalement opensource qui fonctionne avec Linux:
https://www.pine64.org/pinephone/

13) ORDINATEURS

Les mêmes techniques proposées au dessus s'appliquent également pour les ordi.
Un antivirus à jour (malwarebites par exemple) et un pare-feu sont plus que nécessaires pour les utilisateurs de Windows.
Pour vous protéger des virus, on vous conseille de mettre à jour vos applications dès que l'on vous le propose.
Faites également attention aux documents que vous ouvrez sur votre ordinateur notamment sur Windows. Il n'est pas compliqué de mettre un virus dans un fichier PDF ou Word qui infecte votre ordinateur si vous l'ouvrez avec Acrobat ou MS Office. Les applications libres sous Linux comme LibreOffice sont plus résistantes face à ce type d'attaques principalement car il y a moins d'intérêt financier à faire des virus pour Linux. Cela n'empêche pas une attaque ciblée contre une personne utilisant Linux.

Évitez d'utiliser votre ordinateur personnel pour les activités militantes. Privilégiez plutôt un os libre et sécurisé, par ordre de difficulté de prise en main :
- Tails
- Whonix
- Qubes

Si votre ordinateur tombe dans les mains de la police et que vous n'avez rien préparé, ils auront accès à une quantité impressionnante de données sur vous. Cela va même jusqu'aux fichiers que vous avez supprimé si vous n'avez pas pensé à les écraser proprement via des applications spécifiques. Le mot de passe administrateur d'un mac ou d'un Windows ne vous protège absolument pas et le choisir long ne servira qu'à vous protéger d'amis intrusifs n'ayant pas le temps de se renseigner pour les contourner.
Pour ralentir l'obtention de vos données, vous pouvez choisir de chiffrer vos données : Veracrypt ou Luks. Attention cependant, vous ne pourrez faire confiance au chiffrement de vos données via Luks ou Veracrypt que si votre ordinateur est éteint.

À noter que la confiance en veracrypt et luks à baissé ces derniers temps suite à l'affaire des voitures brûlées où Ivan est inculpé[8].
Cependant l'enquête est gardée secrète est c'est possible qu'ils aient récupéré les mots de passe par d'autres méthodes (evil maid attack – voir plus bas -, keylooger, erreur humaine…) plutôt que par force brute ou via une faille de sécurité.
Il reste tout de même fortement conseillé d'actualiser ses chiffrements. **Privilégiez Luks2** (voir partie Tails)

Pour effacer des fichiers, référez-vous au « guide d'autodéfense numérique » à la partie « supprimer des fichier » et sur guide.boum.org

14) TAILS

tails.boum.org
Tails ne peut pas toujours vous protéger s'il est installé depuis un ordinateur infecté par des virus ou si vous l'utilisez sur un ordinateur comportant du matériel malveillant, tels des enregistreurs de frappe (voir plus bas anti evil maid).

8 https://nantes.indymedia.org/posts/87395/une-lettre-divan-enferme-a-la-prison-de-villepinte-perquisitions-et-disques-durs-dechiffres/

Avec Tails, vous pouvez transformer temporairement votre propre ordinateur en une machine sécurisée. Vous pouvez également rester en sécurité en utilisant l'ordinateur d'une autre personne. Tails est un système d’exploitation linux (debian) live, cad qu’il s’utilise depuis une clef usb ou un cd. Plus de raison de s'inquiéter des virus car Tails fonctionne indépendamment du système d'exploitation habituel et n'utilise jamais le disque dur.

Sans Tails, la plupart de vos activités peuvent laisser des traces sur l'ordinateur :

- Les sites web que vous avez visité, même en navigation privée
- Les fichiers que vous avez ouvert, même si vous les avez supprimé
- Les mots de passe, même si vous utilisez un gestionnaire de mots de passe
- Tous les périphériques et réseaux Wi-Fi que vous avez utilisé

À l'inverse, Tails n'écrit jamais sur le disque dur et n'utilise que la mémoire vive de l'ordinateur pour fonctionner. Cette mémoire est effacée intégralement lors de l'extinction de Tails, supprimant ainsi toutes les traces possibles.

Vous pouvez **enregistrer des fichiers et certaines configurations** dans un stockage persistant chiffré (Luks2, excellent chiffrement) sur la clef USB : vos documents, vos marque-pages du navigateur, vos courriers électroniques et même des logiciels supplémentaires.Le stockage persistant est optionnel et vous décidez toujours de quel contenu est *persistant*. Tout le reste est *amnésique*.

Tails est fourni avec une sélection d'applications permettant de travailler sur des documents sensibles et de communiquer en sécurité.
Toutes les applications sont prêtes à l'emploi et leurs paramètres par défaut sont sains afin d'éviter les erreurs.
Logiciels inclus dans Tails :
- Le Navigateur Tor avec uBlock, un navigateur sécurisé et un bloqueur de publicité
- Thunderbird, pour les messages électroniques chiffré
- Kleopatra, pour les clefs pgp
- KeePassXC, pour créer et gérer des mots de passe forts
- LibreOffice, une suite bureautique
- Gimp, éditeur d’images
- OnionShare, pour partager des fichier via Tor
- Un nettoyeur de métadonnées (utilise mat2), suffit de faire click droit – enlever les métadonnées sur un fichier
- et de nombreux autres !

Pour éviter les erreurs :
- Toutes les données du stockage persistant sont chiffrées automatiquement.
- Tails n'écrit rien sur le disque dur. La mémoire vive (ram) est entièrement effacée lors de l'extinction de l'ordinateur.
- Les applications essayant de se connecter à Internet sans passer par Tor sont automatiquement bloquées. Vous pouvez visiter des sites web de manière anonyme ou changer votre identité. Changer votre identité refait un nouveau circuit tor et redémarre le navigateur.
- Prenez soin de ne pas mélanger vos identités sur un même navigateur sur le même circuit tor.

<u>Démarrer tails :</u>

Pour utiliser Tails, éteignez l'ordinateur et démarrez-le sur votre clé USB Tails à la place de Windows, macOS ou Linux. Il est souvent nécessaire d'accéder au BIOS et de modifier depuis quel disque démarre l'ordi. Pour savoir comment accéder au BIOS de votre ordinateur, visitez le site de Tails (tails.boum.org) et aller à la section « Documentation » puis « Premiers pas avec Tails ».

15) Sauvegarde
On a vu plus haut qu'il vaut mieux stocker ses données en local plutôt que sur le cloud.
Grace au stockage persistant de Tails, vous pouvez stocker des documents en toute sécurité à condition d'avoir un mot de passe correct.
A l'aide de l'utilitaire Disques, Tails permet de formater un disque (clefs usb par exemple) et de le chiffrer avec luks2 (click droit sur la clef usb – formater). Attention, le disque ne peut être lu que par des système linux après dévérouillage du mot de passe.
Aussi vous pouvez cloner une clef tails et sauvegarder l'espace persistant sur cette autre clef. En effet, lorsque l'on fait des sauvegardes en local il est nécessaire de faire des backups en cas de perte ou de malfonctionnement d'un disque (les supports de stockage ont tendance à être fragiles et capricieux).
Attention à ne pas mélanger les identités.

16) Effacement des données
Pensez à faire une sauvegarde avant

Quand on met un fichier à la corbeille ou qu'on l'efface explicitement, les systèmes d'exploitation n'effacent pas le contenu du fichier.
À la place, ils effacent simplement l'entrée du fichier du système de fichiers (« l'adresse » du fichier n'existe plus, il n'y a plus le chemin pour y aller). Le contenu du fichier, donc les données, restent sur le support de stockage. Ces données resteront disponibles jusqu'à ce que le système réutilise l'espace pour de nouvelles données.
Méthodes conseillées :
- Détruire physiquement le dispositif.
- Chiffrer l'appareil avant utilisation.
- Nettoyer de manière sécurisée tout le disque. Depuis tails, par exemple, ouvrez l'utilitaire « Disques ». Sélectionnez le périphérique que vous souhaitez effacer. Choisissez « formater le disque » puis « remplacer les données existantes par des zéros ».
- Accéder aux fichiers de son disque depuis tails. Pour se faire, démarrer tails. Selectionner « More options>Yes ». Creer un mot de passe administrateur (sera valable que jusqu'au prochain redémarrage). Dévérouiller et monter le disque à l'aide de l'utilitaire Disques : Applications>Accesoires>Disques

Pour en savoir plus, comment supprimer des fichiers de manière sécurisée ou comment nettoyer l'espace disponible : tails.net/doc/encryption_and_privacy/secure_deletion/index.fr.html
Rdv également sur le site de surveillance self-defense (ssd.eff.org) et chercher « delete ».

Sur smartphone, vous pouvez faire un redémarrage d'usine.

17) Cryptomonnaies
Bitcoin n'est pas anonyme, il enregistre toutes les transactions.
Pour rendre des bitcoins anonymes envoyez-les à un blender (blener.io par ex.) puis sur votre portefeuille sur tails (Electrum Bitcoin Wallet)

Il est préférable d'utiliser Monero qui ne garde rien en mémoire.

Envoyez-les sur votre portefeuil monero sur Tails (voir « Échanger du Monero à l'aide de Feather » sur tails.boum.org).

Acheter des cryptomonnais depuis une banque de crypto
On doit donner toutes ses infos personnelles comme pour une banque (coinbase, binance…).
Ne pas dépenser vos crypto directement depuis l'application d'échange, on ne peux pas leur faire confiance. Les envoyer d'abord sur son portefeuille sur tails.

Acheter des crypto avec un mandat cash.
Le Mandat Versement sur Compte, une option proposée par la Banque Postale.
Il vous permet de déposer la somme que vous souhaitez au guichet, afin que celle-ci soit virée sur n'importe quel compte bancaire de votre choix. Vous êtes limités à 1500 euros par envoi, et cette méthode comporte des frais, qui peuvent aller de 4€90 à 9€40, selon la somme que vous avez choisi d'envoyer.

Pour vous permettre d'obtenir des crypto via cette méthode :
- Dygicode : ce service vous permet de vous procurer des crypto monnaies via un paiement en espèces que vous effectuez dans des bureaux de tabac partenaires. Il s'agit d'une sorte de recharge pré-payée qui vous permet de récupérer vos cryptos via le site officiel digycode.com
- LocalCoinSwap (ou autre plateforme d'échange de crypto-monnaie peer to peer) : il rassemble des particuliers qui acceptent parfois (pas tous attention) les échanges de mandat cash contre des Bitcoins.

Acheter des Bitcoins avec des cartes prépayées
Carte Paysafecard et carte Néosurf
Cette carte permet d'effectuer des achats en ligne en toute simplicité. Vous pouvez vous la procurer, avec le moyen de paiement de votre choix, via du liquide dans notre cas, dans divers endroits tels que les points presse, supermarchés, buralistes, etc...
- LocalCoinSwap : il suffira de trouver un vendeur qui accepte ce moyen de paiement.

Envoyer de l'argent à qqn en échange de cryptos (localcoinswap)

Les distributeurs automatiques de Bitcoins

18) Enlever micros
Pour être sur de ne pas être écouté, il est possible de désactiver ses micros physiquement.
Il existe en général 2 micros par appareil : un principal et un d'ambiance (qui capte les bruits d'ambiance pour les éliminer).
Sur ordi : le plus souvent les micros et la camera se situent dans la partie haute de l'écran. Il faut décoller l'écran délicatement à l'aide d'un petit tourne-visse plat. Vous verrez un câble que vous pourrez débrancher.
Sur smartphone : les micros sont sur la carte mère. Il faut donc regarder la doc de son modèle pour démonter le tel. Il existe souvent des tutos sur youtube. Ensuite il faut repérer les micros (voir doc). Ce sont deux petits composants de 2mm sur 3mm environ. Une fois repérés, leur foutre un coup de fer à souder (en faisant attention à ne pas abîmer le reste).
Vous pouvez toujours brancher des écouteurs et utiliser le micro des écouteurs.

19) Anti Evil Maid

Une attaque de type "evil maid" est une attaque contre un appareil laissé sans surveillance, dans laquelle un attaquant ayant un accès physique modifie l'appareil d'une manière indétectable afin de pouvoir accéder ultérieurement à l'appareil ou aux données qu'il contient.

Le nom fait référence au scénario dans lequel une femme de chambre pourrait subvertir un appareil laissé sans surveillance dans une chambre d'hôtel - mais le concept lui-même s'applique également à des situations telles que l'interception d'un appareil en transit, ou sa confiscation temporaire par le personnel d'un aéroport ou des forces de l'ordre.[9]

Rappel : Éteindre systématiquement ses appareils lorsque l'on s'en sépare ou que l'on est dans une situation à risque (contrôle, aéroport, lieu avec présence policière…)

Si l'appareil est éteint et si le disque est chiffré, alors le micrologiciel (firmware) de l'appareil doit être compromis, généralement à l'aide d'un périphérique externe. Le micrologiciel compromis fournit alors à la victime une fausse fenêtre de demande de mot de passe identique à l'original. Une fois le mot de passe saisi, le micrologiciel compromis se retire après un redémarrage. Pour réussir l'attaque, l'attaquant doit revenir à l'appareil une fois qu'il a été laissé sans surveillance une deuxième fois pour voler les données désormais accessibles.[10]
(Des attaques plus sophistiquées *pourraient* envoyer le mot de passe à l'attaquant par l'intermédiaire du réseau)

Pour s'en protéger nous conseillons :
- Cacher ses appareils lorsque l'on s'en sépare.
- Mettre ses appareils dans un coffre fort ou rangement à clef.
- Systématiquement se tromper de mot de passe une première fois.
- Mettre du vernis à paillettes sur les visses de l'ordinateur. Ensuite prendre en photo. Quand on reviens sur son appareil comparer avec les photos. Le moindre petit changement sera facilement détectable.
- le logiciel open source de BIOS coreboot et la surcouche Heads (https://osresearch.net/) qui permet de détecter un changement à l'aide d'une clef mfa que l'on garde sur soi. Les librem des purism ou les nitropad de nitrokey sont compatibles par exemple.

20) Les attaques liées aux erreurs humaines
- Shoulder surfing
On parle de shoulder surfing quand quelqu'un regarde ce qu'on écrit au-dessus de notre épaule. Aussi si une caméra arrive à voir notre écran.
Faire attention aux caméras, taper ses mots de passe de façon discrète, se mettre dans un coin de pièce quand on est sur notre ordinateur ou notre téléphone. On peut également acheter un filtre de confidentialité, empêche les personnes ne se trouvant pas en face de l'écran de le voir.

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

Le ***phishing*** est une technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, proche...) afin de lui soutirer des renseignements personnels,

9 https://en.wikipedia.org/wiki/Evil_maid_attack
10 https://lwn.net/Articles/651021/

faire lire un fichier corrompu, installer une application malveillante, ou à l'inciter à aller sur un serveur contrôlé par l'attaquant via un lien – ce qui permet le téléchargement de fichiers -.
Même si l'Etat dispose d'attaques « 0 clicks » (pas besoin d'intéraction de la victime par exemple pegasus ou le « hacking van » de Nexa) elles sont rares. Predator, le concurrent français de pegasus fonctionne qu'en « one click ».
Il est important de faire attention lorsque l'on ouvre un fichier dans un message ou lorsqu'on clique sur un lien. Que ce soit mail, sms ou messagerie instantanée. Cela est valable également pour les qr codes !
Nous vous conseillons de :
- ne pas cliquer sur des liens envoyés par sms ou mail, ni d'ouvrir de pièces jointes dans la mesure du possible. (ni lire des qrcodes)
- consulter vos mails sur un profil isolé vide sans privilèges. Voir carrément sur tails sans persistant.
- vérifier l'adresse des liens (en cas de doute vérifier sur whois.com)
- ne pas cliquer sur des liens mais plutôt les copier-coller dans un navigateur sécurisé
- faire attention aux infos partagées

- **Périphériques inconnus :**
Nos appareils ne possèdent pas ou très peu de protection contre les périphériques usb (disque dur, clef usb, câble de chargeur, clavier, souris...). En effet c'est avec eux qu'on communique avec l'ordinateur. Ainsi il est possible qu'un périphérique inconnu inséré dans un appareil injecte du code très rapidement et le compromette (attaques types Ruber Ducky).
Si vous décidez de connecter un périphérique inconnu (disque dur, clef usb, câble de chargeur, clavier, souris…) a un de vos appareils, faites-le d'abord sur une session Tails sans avoir déverrouillé le persistant.