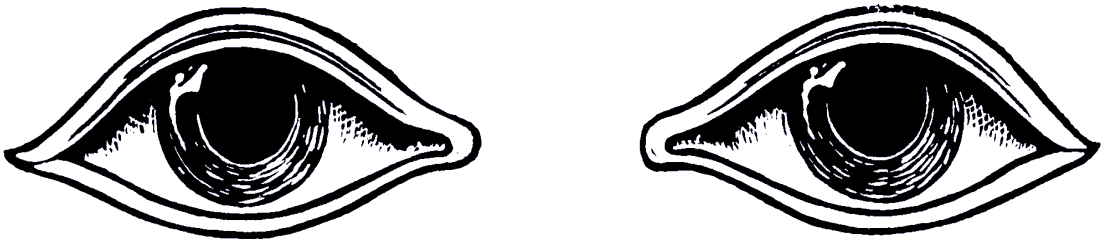


- RIO -

COMMENT VERROUILLER SON TELEPHONE

@xradmin, XR Global Tech / XR International Support, https://rebellion.global

Si vous avez un ordinateur portable, lisez aussi le Laptop Lockdown

Prendre votre téléphone sur une action

Vous avez donc décidé de prendre votre téléphone sur une action. Au préalable, nous devons nous assurer que vous avez pris les précautions nécessaires…

Il est bien peu de téléphones qui contiennent *uniquement* des données appartenant à leur utilisateur : la plupart contiennent de nombreux contacts, photos et vidéos d'autres personnes – celles qui forment notre entourage. Même s'il vous importe peu d'égarer les données de votre téléphone, il est possible que les autres s'en soucient, ou soient mis en difficulté si votre téléphone n'est pas suffisamment protégé contre le vol de données, notamment les personnes pratiquant la désobéissance civile. De plus, si vous coordonnez des actions pour XR, vous possédez probablement une longue liste de contacts qui pourrait être utilisée par un adversaire afin de porter un lourd préjudice à tout le groupe d'action. D'importants identifiants de connexion peuvent également être détournés ou compromis.

Expérience : se détacher de son téléphone

Dans un lieu calme, posez votre téléphone sur une table devant vous, écran tourné vers le bas. Ne le touchez plus, regardez-le. Imaginez que ce téléphone soit confisqué par un policier. Imaginez que vous ne verrez plus jamais ce téléphone, qu'il sera disséqué au commissariat par des experts qui copieront vos photos et vidéos (si c'est un téléphone récent), tous vos contacts, textos, ouvriront le navigateur et se connecteront à vos comptes sur les réseaux sociaux et la Base XR. Peut-être aussi prendront-ils votre carte MicroSD.

Réfléchissez, non seulement à la *chose* qu'est ce téléphone, mais aussi aux *gens* auxquels il conduit, et à quels *comptes* (et informations) il permet de se connecter. Pensez aussi à la façon dont la situation pourrait impliquer d'autres rebelles, non seulement sur cette action, mais aussi plus tard, même quand ces personnes ne feront plus partie du mouvement.

En somme, **on ne verrouille pas son téléphone pour soi seul, mais aussi pour prendre soin de son entourage**. Notre culture régénératrice implique un certain respect de la vie privée et de l'anonymat, dans une époque où ces droits fondamentaux sont massivement exploités par les entreprises et les gouvernements pour contrôler, affaiblir et condamner.

SOYEZ ATTENTIF AUX DONNÉES SUIVANTES

- Photos, vidéos et enregistrements de rebelles, particulièrement aux réunions d'action
- Comptes liés à XR (Mattermost, Base, email, Pads, etc.)
- Listes de contacts

Demandez-vous :

« Est-ce que j’ai *besoin* de prendre mon téléphone sur cette action ? »

Téléphones à l’ancienne

Les vieux téléphones sont très difficiles à sécuriser car ils ne permettent pas de chiffrer eux-mêmes leurs données. Ceci dit, leur stockage et leurs usages sont si limités qu’ils contiennent généralement beaucoup moins d’informations que les appareils récents.

IMPORTANT : Extraire les contacts et informations d’un vieux téléphone est très simple. Assurez-vous d’avoir effacé tous les contacts du téléphone et de la carte SIM, et de n’y garder que ceux qui sont utiles pour l’action.

« Smartphones »

Sécuriser les « iPhones » par le chiffrement

La plupart des téléphones Apple (iOS) récents chiffrent automatiquement leur contenu. Mais cela n’empêche pas une personne en possession de votre téléphone d’accéder à ses données. C’est pourquoi le chiffrement doit être protégé par un mot de passe, sans lequel les données restent inaccessibles.

IMPORTANT : Si vous choisissez un mot de passe composé uniquement de chiffres, un pavé numérique apparaîtra sur l’écran de déverrouillage, ce qui est plus pratique que de taper une suite de lettres et de symboles sur un petit clavier virtuel. Toutefois, nous conseillons de choisir un mot de passe alphanumérique qui dépasse 8 caractères, car il sera bien plus difficile à casser, bien que les appareils Apple soient conçus pour ralentir les logiciels d’intrusion.

iOS4 à iOS7

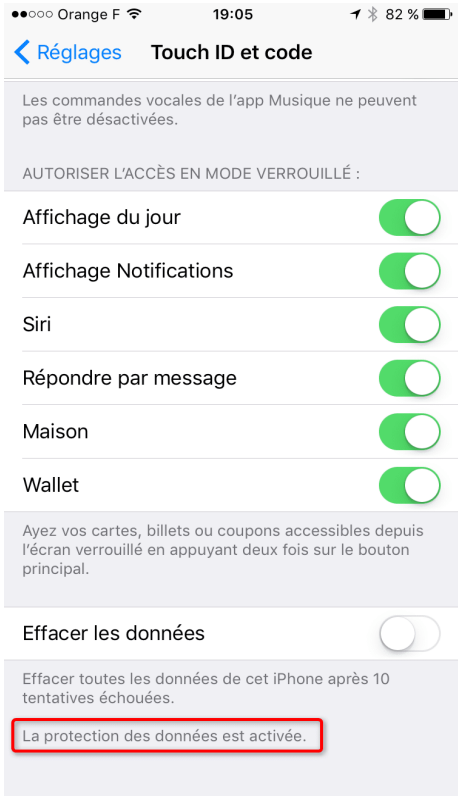
1. Ouvrez les Réglages et choisissez Passcode (ou iTouch & Passcode).
2. Suivez les instructions pour créer un code.

iOS8 et suivants

Si votre appareil utilise iOS8, désactivez le Code Simple pour créer un code qui dépasse 4 chiffres. Depuis la sortie d’iOS9, les codes contiennent 6 chiffres par défaut.

Pour personnaliser votre code, sélectionnez « Changer le code » puis « Code alphanumérique personnalisé ». Vous devez aussi régler l’option « Exiger le code » sur « immédiatement » pour que votre appareil ne soit pas déverrouillé quand vous ne l’utilisez pas.

Après avoir défini un code, descendez tout en bas de la page « Touch ID et code ». Vous devriez lire « La protection des données est activée. » Cela indique que le chiffrement de l'appareil est maintenant lié à votre code, et que l'accès à la plupart des données de votre téléphone nécessitera ce code.



Attention aux sauvegardes sur « cloud » proposées par Apple

Les appareils Apple effectuent généralement des sauvegardes à distance, sur iCloud ou iTunes.

IMPORTANT: Toutes les données que vous transférez sur iCloud doivent être considérées comme accessibles à la police. Même si Apple assure que toutes les données y sont chiffrées, ils disposent eux-mêmes des clés, et sont obligés de coopérer avec les procédures judiciaires dans le cas d'une enquête criminelle. C'est pourquoi cette option doit être évitée.

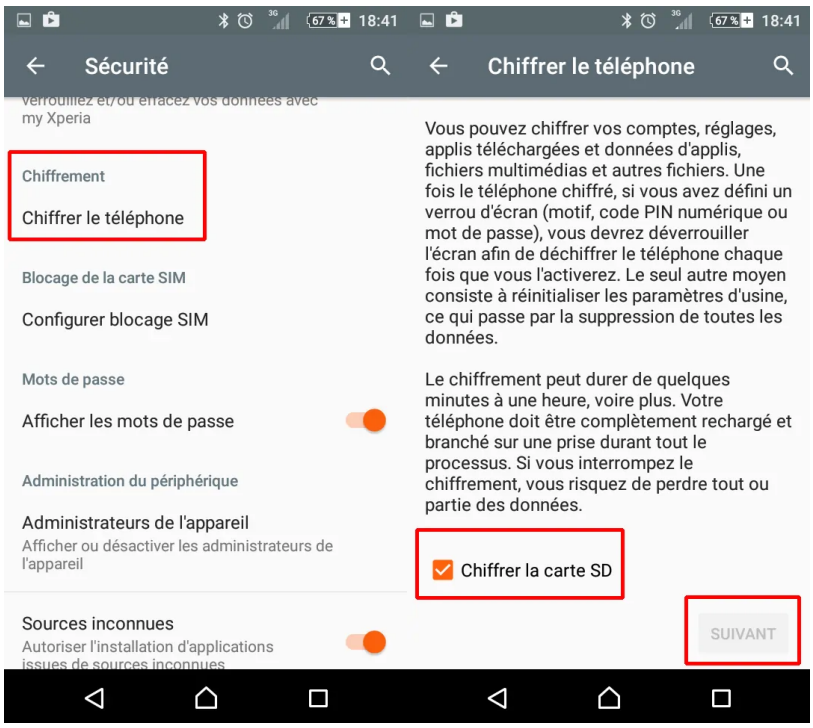
Si vous avez une copie des données de votre téléphone sur votre ordinateur en passant par iTunes, sachez que le système de sauvegarde d'iTunes ne chiffre pas les données par défaut. Vous devez donc activer l'option *Chiffrer la sauvegarde* pour que toutes les données soient chiffrées lors de leur stockage dans votre ordinateur. Assurez-vous de bien mémoriser le mot de passe que vous choisissez, et d'activer le chiffrement intégral du disque dur de votre ordinateur.

Sécuriser les téléphones Android par le chiffrement

Le chiffrement fonctionne à peu près de la même manière sur tous les appareils Android, mais les méthodes pour l'activer ont un peu changé au cours des années. Aujourd'hui, la plupart des appareils sont chiffrés par défaut, notamment ceux qui utilisent une version récente d'Android. Par exemple, tous les Pixel, les Nexus 6P, Nexus 5X, et même les Nexus 6 et Nexus 9 sont chiffrés par défaut. Pour les autres, la marche à suivre est très simple.

Android 5.0 et suivants

Pour les téléphones et tablettes utilisant Android 5.0 Lollipop ou une version plus récente, rendez-vous directement dans le menu « Sécurité » des paramètres. Y parvenir peut changer un peu selon les fabricants, mais la version native d'Android présente les choses ainsi : Paramètres > Confidentialité > Sécurité.



Là, vous trouverez une option pour *Chiffrer le téléphone*. Il vous sera demandé de brancher votre téléphone sur secteur pendant le processus, pour éviter qu'il ne s'éteigne et ne provoque des erreurs. Si ce n'est pas déjà fait, il vous sera demandé d'activer un écran de verrouillage avec code PIN ou mot de passe, lequel devra être saisi quand vous allumerez en déverrouillerez votre téléphone pour accéder aux fichiers nouvellement chiffrés.

Android 4.4 et précédents

Si votre téléphone utilise Android 4.4 KitKat ou une version antérieure, vous devez configurer un PIN ou un mot de passe avant de procéder au chiffrement. C'est très simple : allez dans Paramètres > Sécurité > Écran de verrouillage. Là, vous pouvez choisir un schéma, un PIN ou un mot de passe. Le même code devra être utilisé après le chiffrement, donc retenez-le bien.

Après quoi, retournez au menu Sécurité et sélectionnez « Chiffrer le téléphone » ou « Chiffrer la tablette ». Vous devez ensuite brancher votre téléphone, lire les avertissements, et probablement confirmer votre code une dernière fois avant que le processus de chiffrement ne commence.

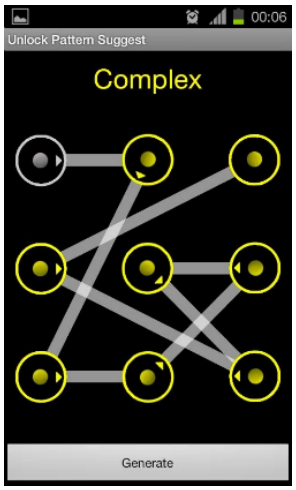
Chiffrer un téléphone peut prendre une heure, voire plus, selon sa puissance et la quantité de données qu'il contient. Quand le processus est terminé, vous pouvez entrer votre PIN et l'utiliser.

Dans le menu *Sécurité*, vous trouverez aussi une option pour chiffrer les fichiers de votre carte microSD. Ceci est recommandé pour sécuriser toutes vos données. Notez qu'après avoir été chiffrée, cette carte microSD ne sera utilisable sur aucun autre appareil (comme votre ordinateur ou appareil photo).

Schéma de déverrouillage pour téléphone Android

Un mot de passe assez solide peut être difficile à retenir, ce qui pousse les gens à utiliser des codes plus courts et moins sûrs. Mais sur tous les téléphones Android, il existe l'option du Schéma de déverrouillage. C'est une excellente option, car généralement les gestes complexes se mémorisent plus facilement que les longs mots de passe. Assurez-vous que le schéma comporte au moins 6 lignes, et essayez d'utiliser une grille de 4x4 ou plus.

Une grille de 3x3 peut être fiable, à condition que le schéma soit suffisamment complexe. Ci-dessous un exemple.



Attention aux sauvegardes sur « cloud »

Les appareils Android se synchronisent avec diverses sauvegardes à distance. Toutes doivent être désactivées et remplacées par une sauvegarde sur un appareil local, lequel doit être complètement chiffré. Un guide pour la sécurité des ordinateurs sera disponible prochainement. Avant de se rendre dans une action, les options comme le « SideSync » de Samsung doivent être désactivées.

IMPORTANT : Si vous êtes développeur, désactivez le débogage USB. Les développeurs et bidouilleurs utilisent souvent des moyens particuliers pour modifier légèrement leurs téléphones. Si par exemple le *Débogage USB* est activé, le risque existe qu'un intrus, à l'aide d'un accès physique à l'appareil, puisse utiliser les outils de débogage d'Android pour consulter vos données. Assurez-vous que le *Débogage USB* soit désactivé sur votre téléphone avant de le prendre sur une action !

Cartes MicroSD

Les cartes MicroSD peuvent facilement être extraites du téléphones, leurs données analysées et copiées. Passez en revue tout le contenu d'une carte avant de l'emmener en action. Considérez que tout ce qu'elle contient est vulnérable.

IMPORTANT: Même si votre téléphone est chiffré, votre MicroSD ne l'est probablement pas. Certains téléphones permettent de chiffrer une carte MicroSD. Assurez-vous que votre carte ne contient aucune donnée sensible avant de l'emmener en action, à moins qu'elle ne soit chiffrée.

Communiquer sans risque avant & pendant les actions

Deux types de réseaux

Il existe actuellement deux grandes façons de communiquer vocalement et textuellement avec un téléphone : les SMS et appels vocaux utilisant le réseau mobile traditionnel (GSM, CDMA), ou la communication par internet à l'aide d'applications, des réseaux 3g, 4g, ou d'une connexion WiFi.

Sur une action, il est rare de disposer d'une connexion WiFi. En général, on utilise une carte SIM pour se connecter à un réseau mobile (que ce soit pour appeler ou envoyer des SMS), ou bien le réseau 3g ou 4g avec une application (comme *Signal*, *Telegram* ou *WhatsApp*).

Une carte SIM est comme une plaque d'immatriculation : liée à une identité, souvent à un compte bancaire via l'abonnement téléphonique, elle est un moyen très rapide d'identifier une personne, et ce à travers une simple consultation, sans même que la police ait à accéder aux serveurs de l'opérateur.

Il est donc recommandé d'utiliser une SIM jetable. Elles peuvent être achetées en espèces, sans que votre identité ne soit tracée. Elles compliquent grandement la tâche des services de surveillance s'ils cherchent à associer vos communications avec une personne. Les SIM jetables peuvent être achetées en espèces et sans pièce d'identité dans de nombreux pays, mais pas tous. En Allemagne par exemple, Lycamobile propose ce type de carte en magasin. Aidez vos camarades à utiliser une SIM jetable, et protégez votre SIM avec un code, si possible.

Encore mieux : utiliser une SIM jetable avec un téléphone jetable (ou un téléphone d'occasion acheté en espèces). Ainsi, l'identité du téléphone, l'IMEI, ne peut pas non plus vous être associée. Dans l'idéal, tous les coordinateurs d'action doivent envisager le combo téléphone+SIM jetables. Pour plus d'infos, consultez ce post sur la Global Base.

IMPORTANT : Évitez de passer des appels ou d'envoyer des SMS (textos) liés à XR en utilisant le réseau mobile, sauf en cas d'absolue nécessité. Si toutefois vous le faites, ne donnez jamais aucun détail qui puisse incriminer ou identifier qui que ce soit.

Appeler sans risque avec le chiffrement End to End (e2e)

Le chiffrement End-to-end désigne un type de confidentialité par lequel les données ne sont lisible par aucun autre appareil que celui auquel les données sont destinées. Personne ne peut les intercepter. Il existe plusieurs applications permettant les appels et textos en e2e. *Toutes nécessitent que votre destinataire ait installé l'application, et que vous l'ayez préalablement ajouté au carnet d'adresses de cette application.*

IMPORTANT : WhatsApp et Telegram sont peu fiables. Ces deux applications ont de graves problèmes de sécurité. Nous conseillons de n'utiliser que Signal ou Wire pour communiquer sans risque sur une action.

Signal (OpenWhisperSystems)

Signal a une excellente réputation dans les milieux de la sécurité informatique, et son utilisation est de plus en plus répandue. Son adoption rapide est notamment due à la façon dont elle utilise les numéros de téléphone des utilisateurs pour les mettre en contact. Vous pouvez ainsi entrer le numéro de téléphone d'un·e ami·e et l'inviter à rejoindre Signal. Vous pouvez aussi découvrir, à travers l'appli, ceux de vos contacts qui l'utilisent déjà.

Signal permet les discussions de groupe, les appels vocaux et vidéo, et occupe une place centrale dans les communications internes de nombreux groupes XR.

Le système reposant sur les numéros de téléphone n'est toutefois pas sans risque pour les activistes. Si votre téléphone est compromis et/ou insuffisamment sécurisé, il est aisé pour un adversaire de découvrir les personnes avec lesquelles vous avez communiqué via Signal.

IMPORTANT : Si vous choisissez d'utiliser Signal, connectez-le au numéro d'une carte SIM jetable (achetée en espèces et sans pièce d'identité), si possible. Aussi, utilisez l'option *Verrouillage de l'écran* proposée par l'appli, afin de compliquer davantage la tâche de ceux qui voudraient accéder à votre liste de contacts.

Vous pouvez télécharger Signal pour iOS et Android ici. Notez qu'il existe aussi une version pour ordinateur, très pratique si vous travaillez à cheval entre votre téléphone et votre ordinateur.

IMPORTANT: N'installez Signal sur votre ordinateur que si celui-ci est suffisamment sécurisé, car tous vos contacts et messages y seront accessibles.

Wire

Contrairement à Signal, Wire ne dépend pas d'une carte SIM pour être activée. Elle n'est pas mieux chiffrée que Signal, mais offre un meilleur potentiel d'anonymat. Wire permet la discussion, les appels vocaux et vidéo, et le partage de fichiers. Atout assez unique : l'application autorise plusieurs comptes sur un seul téléphone.

Un des inconvénients de Wire et qu'il est utilisé par beaucoup moins de gens que Signal. Ceci est notamment dû au fait que Signal a proposé une version stable beaucoup plus tôt. Un autre inconvénient est qu'il est impossible d'y ajouter un schéma de verrouillage ou autre code pour protéger son contenu d'intrus qui auraient accès à votre téléphone allumé.

Wire tourne sur iOS 10.0 ou Android 5.0 et toutes versions ultérieures. Si votre appareil est plus ancien et ne peut pas être mis à niveau, optez pour Signal. Notez qu'il existe aussi une version pour ordinateur, très pratique si vous travaillez à cheval entre votre téléphone et votre ordinateur.

IMPORTANT: N'installez Wire sur votre ordinateur que si celui-ci est suffisamment sécurisé, car tous vos contacts et messages y seront accessibles.

Wire est disponible ici.

Briar

Briar est le dernier-né dans cette constellation de la contre-surveillance téléphonique, et propose certainement l'offre la plus unique. Contrairement à toutes les autres solutions de messagerie chiffrée en e2e, Briar ne dépend pas de l'infrastructure réseau traditionnelle pour fonctionner. Créée pour les activistes, l'application prévoit les situations où l'État aurait désactivé et/ou brouillé les réseaux

téléphoniques ou WiFi aux alentours d’une action ou d’une manifestation, comme cela a été largement documenté, notamment en Turquie, Chine, Ukraine, ou encore aux États-Unis.

Pour ce faire, Briar mobilise la fonctionnalité Bluetooth de presque tous les téléphones pour passer le message d’appareil en appareil et former un maillage : un avantage considérable dans le cas d'un effort coordonné visant à désactiver l'infrastructure de communication d'une action prolongée (à condition que la police n’ait pas physiquement accès à tous les participants et ne puisse tout simplement saisir leurs appareils).

Lorsqu’une connexion internet est disponible, Briar anonymise les communications à travers le Réseau Tor, ajoutant ainsi une couverture supplémentaire puisqu’il devient impossible de prouver les liens établis entre deux appareils.

> Briar est disponible ici.

Sécuriser l’accès au téléphone

Une des meilleures manières de « penser sécurité » est d’imaginer votre appareil entre les mains d’un adversaire capable de vous incriminer, ou d’incriminer tout ou partie du groupe dont vous faites partie.

Règles pour tous les « smartphones »

1. NE RÉUTILISEZ PAS UN MOT DE PASSE UTILISÉ AILLEURS

Si vous utilisez les identifiants de votre compte bancaire pour déverrouiller votre téléphone, et qu’un agent des renseignements a un mandat pour accéder à toutes vos données bancaires (ce qui est très courant), la police peut déverrouiller votre téléphone. C’est pourquoi il est toujours préférable d’utiliser un mot de passe différent, dans la mesure où vous préférez le mot de passe au schéma (Android). Choisissez un mot de passe d’au moins 9 caractères, et alpha-numérique si possible.

2. N’UTILISEZ PAS L’IDENTIFICATION BIOMÉTRIQUE (EMPREINTE DIGITALE OU RECONNAISSANCE FACIALE)

En état d’arrestation, il ne fait aucun doute que la police aura accès à votre corps et pourra, sous la contrainte, l’utiliser pour accéder à votre appareil si celui-ci est verrouillé avec vos données biométriques. En France, il est déjà arrivé que les téléphones de rebelles soient déverrouillés par les policiers, tout simplement en forçant le visage du rebelle à se placer en face du téléphone. De même pour les empreintes digitales. Ces méthodes de verrouillage sont donc à éviter pour les activistes.

3. NE STOCKEZ JAMAIS DE MOTS DE PASSE NON-CHIFFRÉS, NI EN LOCAL NI DANS LE « CLOUD ». STOCKEZ-LES CHIFFRÉS ET/OU DANS VOTRE TÊTE

Il est pratique d’avoir un pense-bête pour les mots de passe de votre téléphone, mais il devient beaucoup moins pratique que vos adversaires y aient accès. N’utilisez pas de services comme *LastPass* ou *1Password*, qui stockent vos codes sur des serveurs dans lesquels une seule intrusion pourrait s’avérer catastrophique et compromettre d’innombrables utilisateurs. Quand l’entreprise 1Password assure qu’il lui est impossible de déchiffrer les mots de passe qu’elle stocke, cela n’engage que ceux qui y croient. Et revient à placer sa sécurité entre les mains de parfaits inconnus. Ces entreprises obéissent aux lois d’un autre pays, où les autorités et renseignements fédéraux ont toute latitude pour les contraindre à coopérer.

Préférez l’utilisation d’un gestionnaire de mots de passe hors-ligne, comme KeePass ou KeePassXC, qui stocke les codes chiffrés sur votre appareil, le tout sous votre contrôle.

Rien ne s’oppose à ce que vous stockiez les codes de votre téléphone sur votre ordinateur, à condition que celui-ci utilise un moyen sûr de les stocker.

Précautions avant arrestation pour chaque groupe

1. NE LAISSEZ PAS LES ADMINISTRATEURS RÉSEAU OU SYSTÈME ALLER EN ACTION

Au risque de décevoir les administrateurs réseau et système, ils doivent savoir qu'ils sont des cibles de très grande valeur pour la police, et seront sujets à de très sévères pressions et/ou incarcérations en cas d'arrestation. **Il est particulièrement défendu aux administrateurs système de se rendre en action.** De plus, un admin en prison n'est plus disponible pour son groupe, ce qui peut être désastreux pour les actions. Les administrateurs système et réseau doivent être en ligne tout au long de l'action pour aider aux verrouillages (*cf.* point suivant).

2. DÉSIGNEZ DES CONTACTS DE VERROUILLAGE

Chaque groupe doit désigner un ou plusieurs contacts de verrouillage dont les détails de contact anonymisés doivent être à la disposition de chaque téléphone emmené en action. **Le rôle de ces rebelles est d'assurer que les administrateurs sachent immédiatement quelles sont les personnes arrêtées, afin qu'ils fassent expirer toutes leurs sessions de connexion et changent leurs mots de passe.** Les contacts de verrouillage doivent être dans un endroit sûr et disposer d'une bonne connexion internet. Ils doivent rester joignables pendant toute l'action.

Il revient à chaque groupe de définir son propre protocole pour le verrouillage des comptes.

3. DÉSIGNEZ DES PORTEURS DE TÉLÉPHONE

Avec l'équipe Action & Logistique, discutez l'éventualité d'avoir des porteurs de téléphones qui documentent, coordonnent et diffusent l'action sur les réseaux sociaux, etc. Cela dissuade les autres rebelles d'emmener leur téléphone, et peut être un bon moyen de minimiser les risques de compromission ou de fuite des données entre de mauvaises mains.

4. ÉTUDIEZ LA LOI

Chaque groupe d'action doit désigner une équipe légale pour travailler *spécifiquement* sur les droits des rebelles au moment de l'arrestation. **Les rebelles ne peuvent pas être sereinement arrêtés s'ils ignorent leurs droits.** Un·e rebelle ne sachant pas qu'il est illégal d'être forcé·e physiquement ou menacé·e dans le but d'obtenir ses identifiants numériques cédera probablement aux demandes. Prendre soin les uns des autres consiste aussi à s'assurer que nous sommes tous dans le même bateau, que nous pouvons avoir fermement confiance en la connaissance de nos droits, et que nous sommes imperméables aux mensonges qui compromettent la sécurité de nos camarades.

IMPORTANT: il est très important de vérifier si, sur votre territoire, refuser de donner ses identifiants à la police pendant votre arrestation contrevient à la loi. Si oui, il est fondamental que tous les

rebelles le sachent, et qu'aucun appareil contenant des données sensibles, chiffrées ou pas, ne soit emmené en action. Refuser de donner des informations aux forces de l'ordre – « entrave à la justice » – est généralement un chef d'accusation bien plus grave que de bloquer une route, et peut déboucher selon les territoires sur plusieurs années d'emprisonnement, voire pire.

Précautions avant arrestation pour chaque rebelle

1. NE TENTEZ D'APPELER PERSONNE, MÊME PAS VOTRE CONTACT DE VERROUILLAGE, À MOINS D'AVOIR BEAUCOUP DE TEMPS

Ce qu'on entendra par « beaucoup de temps » est bien sûr terriblement subjectif, mais tant que vous avez du temps, n'hésitez pas à passer cet appel. Sinon, passez à l'étape 2.

2. ÉTEIGNEZ VOTRE TÉLÉPHONE ET ASSUREZ-VOUS QU'IL SOIT BIEN ÉTEINT AVANT DE LE DONNER

S'il vous est permis de penser qu'il existe le moindre risque que votre téléphone tombe entre les mains de la police ou d'enquêteurs, soyez absolument certain·e de l'éteindre. **Un téléphone chiffré n'est vraiment (pratiquement) invulnérable qu'à condition d'être éteint.** Faites de même si vous traversez une frontière.

3. ÉNONCEZ VOS DROITS

Ce n'est pas forcément facile lorsqu'on se fait emmener, mais essayez de récapituler vos droits dans votre tête. Énoncez-les pour vous-même avant de dire quoi que ce soit à la police.

IMPORTANT: Si la police vous rend votre téléphone et si celui-ci n'est pas chiffré, il doit être considéré comme compromis et donc complètement effacé. Les logiciels malveillants infiltrés dans les téléphones d'activistes sont de plus en plus courants, et permettent aux enquêteurs de vous espionner en activant votre micro ou en copiant les données de votre téléphone.

Laisser votre téléphone à la maison ?

Vous avez donc décidé de laisser votre téléphone à la maison. Bien joué ! Non seulement vous ne risquez pas de le remettre à la police, mais aucun de vos identifiants et contacts n'est exposé à ceux qui pourraient l'utiliser contre vous et/ou d'autres rebelles. Pensez quand-même à chiffrer votre appareil. Les arrestations post-action sont une réalité, et chiffrer un téléphone rend son contenu inaccessible à toute personne qui s'en emparerait, à condition que le téléphone soit éteint.

* * *

Ce guide est encore en construction. Il est seulement destiné à protéger les rebelles qui sont en première ligne sur les actions et leurs préparations.

Le chiffrement du trafic par VPN, les dispositifs contre le pistage et le XSS, le Stingray et la détection par tour de relais, les applis d'anonymat comme Orfox, les systèmes d'exploitation comme LineageOS avec MicroG pour dégoogliser les usages, le nettoyage de l'EXIF, etc., dépassent la portée du présent document, lequel s'adresse aux néophytes. Ils seront traités sur la Global Base, dans la catégorie Operational Security.

Si vous voulez suggérer des ajouts ou des corrections, n'hésitez pas à les publier sur ce fil de la Global Base. Si vous n'êtes pas inscrit sur ce forum, écrivez à support@organise.earth et demandez une invitation à la XR Global Support Team.